НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Інститут телекомунікаційних систем

Кафедра Телекомунікаційних систем

«На правах рукопису»
УДК _____

«До захисту допущено»
Завідувач кафедри
____ _____ Л.О. Уривський
«___»_____20__ р.

Магістерська дисертація

на здобуття ступеня магістра

зі спеціальності 172 Телекомунікації та радіотехніка

на тему: «Дослідження методик підвищення економічних та експлуатаційних показників системи моніторингу Nagios для оператору зв'язку»

Виконала:
студентка ІІ курсу, групи ТС-71мп
Воронюк Марія Миколаївна _____

Керівник:
Доцент кафедри ТС
доцент Гаттуров Віктор Кавич _____

Рецензент:

_____

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент (-ка) _____

Київ – 2018 року

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Інститут телекомунікаційних систем

Кафедра Телекомунікаційних систем

Рівень вищої освіти – другий (магістерський) за освітньо-професійною програмою

Спеціальність (спеціалізація) – 172 «Телекомунікації та радіотехніка» (172.3620.1 «Телекомунікаційні системи та мережі»)

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ Л.О. Уривський

«___»_____20__ р.

ЗАВДАННЯ
на магістерську дисертацію студенту

Воронюк Марії Миколаївні

1. Тема дисертації «Дослідження методик підвищення економічних та експлуатаційних показників системи моніторингу Nagios для оператору зв'язку», науковий керівник дисертації Гаттуров Віктор Кавич доцент кафедри ТС, доцент, затверджені наказом по університету від «___»_____ 20__ р. №_____

2. Термін подання студентом дисертації: 7 грудня 2018 року

3. Об’єкт дослідження система моніторингу Nagios мережі провайдера телекомунікаційних послуг.

4. Предмет є надійність функціонування веб-монітору Nagios при різних реалізаціях.

5. Перелік завдань, які потрібно розробити:

- огляд інформації про центри обробки даних;
- дослідження існуючих систем моніторингу;
- дослідження системи моніторингу Nagios та її архітектури;
- огляд оноплатного комп’ютера Raspberry Pi;

- реалізація системи моніторингу Nagios на центральному вузлі - Raspberry Pi ;
- реалізація системи моніторингу Nagios на центральному вузлі – сервері HP Proliant DL120 G5;
- дослідження економічних та експлуатаційних показників системи моніторингу при різних реалізаціях.

6. Орієнтовний перелік графічного (ілюстративного) матеріалу

Плакат №1 «Тема, мета та завдання магістерської дисертації»

Плакат №2 «Актуальність та постановка задачі»

Плакат №3 «Реалізація макетів»

Плакат №4 «Порівняння економічних та експлуатаційних характеристик при різних реалізаціях Nagios»

Плакат №5. «Висновки»

7. Орієнтовний перелік публікацій

1) Використання та методи підвищення економічних показників системи моніторингу Nagios для оператору зв’язку – збірник матеріалів конференції «Проблеми телекомунікацій – 2018»

8. Дата видачі завдання 10 вересня 2017 р.

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка
1	Пошук джерел інформації та їх систематизація	01.09.2017- 31.04.2018	
2	Огляд інформації про центри обробки даних	10.05.2018 - 29.05.2018	
3	Дослідження існуючих систем моніторингу	01.06.2018 – 30.07.2018	
4	Дослідження системи моніторингу Nagios та її архітектури та огляд оноплатного комп’ютера Raspberry Pi	01.08.2018 – 31.08.2018	
5	Реалізація системи моніторингу Nagios на центральному вузлі - Raspberry Pi	01.09.2017 – 30.09.2018	
6	Реалізація системи моніторингу Nagios на центральному вузлі – сервері HP Proliant DL120 G5	01.10.2018 – 31.10.2018	
7	Дослідження економічних та експлуатаційних показників системи моніторингу при різних реалізаціях	01.11.2018 – 15.11.2018	
8	Вступ, висновки та оформлення роботи	16.11.2018 – 3.12.2018	

Студент Воронюк М.М.

Науковий керівник дисертації Гаттуров В.К.

РЕФЕРАТ

Робота містить 81 сторінок, 29 рисунків, 6 таблиці, 7 лістингів, 19 посилань.

Темою магістерської дисертації є дослідження методик підвищення економічних та експлуатаційних показників системи моніторингу Nagios для оператору зв’язку.

Актуальність теми. Тема магістерської дисертації є актуальною, так як через зростаючі вимоги кінцевого користувача до безперебійного доступу до мережі провайдери телекомунікаційних послуг змушені приділяти велику увагу системам моніторингу мережі, що дає змогу вчасно виявити та швидко ліквідувати проблеми .

Мета дисертації полягає в визначенні можливості встановлення веб-монітору Nagios на комп’ютер Raspberry Pi, дослідження економічних та експлуатаційних показників Nagios при такій реалізації. Проведено порівняння запропонованої реалізації та вже існуючих. Створено робочий макет системи моніторингу для дата-центру на основі одноплатного комп`ютера з запропонованою архітектурою. Описано та обґрунтовано перелік технічних та програмних засобів, що використовуються під час створення макету.

Відповідно до поставленої мети були сформульовані такі **завдання**:

- дослідження системи моніторингу Nagios та її архітектури;
- реалізація системи моніторингу Nagios на центральному вузлі - Raspberry Pi ;
- реалізація системи моніторингу Nagios на центральному вузлі – сервері HP Proliant DL120 G5;
- дослідження економічних та експлуатаційних показників системи моніторингу при різних реалізаціях.

Об’єктом дослідження є система моніторингу Nagios мережі провайдера телекомунікаційних послуг.

Предметом дослідження є надійність функціонування веб-монітору Nagios при різних реалізаціях.

У дисертації була запропонована реалізація програми Nagios на комп’ютері Raspberry Pi, розглянуто стандартну реалізацію програми Nagios на серверах. Було проведено дослідження економічних та експлуатаційних показників при різних реалізаціях системи моніторингу.

Проблематика. Намагання підвищити економічні показники реалізації системи моніторингу стикається з проблемою технічних показників (завантаженості ЦП) машини на якій вона реалізовується.

Апробація результатів дисертації. Основні положення і результати дисертаційної роботи знайшли своє відображення на Одинадцятій міжнародній науково-технічній конференції "ПРОБЛЕМИ ТЕЛЕКОМУНІКАЦІЙ", Дванадцятій міжнародній науково-технічній конференції "ПРОБЛЕМИ ТЕЛЕКОМУНІКАЦІЙ", XVII Всеукраїнській студентській науково-практичній конференції “Innovations in Science and Technology”

Публікації. Основні положення і результати дисертаційної роботи знайшли своє відображення на Одинадцятій міжнародній науково-технічній конференції "ПРОБЛЕМИ ТЕЛЕКОМУНІКАЦІЙ", Дванадцятій міжнародній науково-технічній конференції "ПРОБЛЕМИ ТЕЛЕКОМУНІКАЦІЙ", XVII Всеукраїнській студентській науково-практичній конференції “Innovations in Science and Technology”

Ключові слова: система моніторингу Nagios, Raspberry Pi, сервер, завантаженість центрального процесору, утиліта htop.

ABSTRACT

The work contains pages 81, 29 images, 6 table, 7 listing, 19 references.

The topic of the master thesis is the study of methods for increasing the economic and operational parameters of the Nagios monitoring system for the communication operator.

Actuality of theme. The topic of the master's thesis is relevant, as due to the growing demands of the end-user to uninterrupted access to the network, telecommunication service providers are forced to devote a lot of attention to network monitoring systems, which enables them to identify and quickly eliminate problems in a timely manner.

The purpose of the dissertation is to determine the possibility of installing a Nagios web monitor on a Raspberry Pi computer, studying the economic and operational performance of Nagios in such a realization. Comparison of the proposed implementation and existing ones. The working model of the monitoring system for the data center was created on the basis of a single-payment computer with the proposed architecture. The list of technical and software tools used during the creation of a layout is described and grounded.

In accordance with the stated goal, the following **objectives** were formulated:

- Research of Nagios monitoring system and its architecture;

- implementation of the Nagios monitoring system at the central node - Raspberry Pi;

- implementation of the Nagios monitoring system at the central node - the HP Proliant DL120 G5 server;

- research of economic and operational indicators of the monitoring system under different implementations.

The object of the research is the monitoring system of Nagios network provider of telecommunication services.

The subject of the study is the reliability of the Nagios web monitor operation at various implementations.

The dissertation proposed the implementation of the Nagios program on the Raspberry Pi computer, and discussed the standard implementation of Nagios on the servers. The study of economic and operational indicators was carried out at various monitoring system implementations.

Problems. Attempts to increase the economic performance of monitoring system faced with the problem of technical indicators (CPU load) of the machine on which it is implemented.

Approbation of the results of the dissertation. The main provisions and results of the dissertation work were reflected at the Eleventh International Scientific and Technical Conference "PROBLEMS OF TELECOMMUNICATIONS", the Twelfth International Scientific and Technical Conference "PROBLEMS OF TELECOMMUNICATIONS", the 16th All-Ukrainian Student Scientific and Practical Conference "Innovations in Science and Technology"

Publications. The main provisions and results of the dissertation work were reflected at the Eleventh International Scientific and Technical Conference "PROBLEMS OF TELECOMMUNICATIONS", the Twelfth International Scientific and Technical Conference "PROBLEMS OF TELECOMMUNICATIONS", the 16th All-Ukrainian Student Scientific and Practical Conference "Innovations in Science and Technology"

Keywords: Nagios monitoring system, Raspberry Pi, server, CPU utilization, htop utility.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ 11
ВСТУП 12
РОЗДІЛ 1. ЗАГАЛЬНИЙ ОГЛЯД ЦЕНТРІВ ОБРОБКИ ДАНИХ ТА СИСТЕМ МОНІТОРИНГУ 14
1.1 Загальні відомості про ЦОД 14
1.2 Склад ЦОД 14
1.3 Топологія ЦОД 16
1.4 Основні недоліки ЦОД 19
1.5 Висновки до розділу 1 20
РОЗДІЛ 2. РОЗГЛЯД СИСТЕМ МОНІТОРИНГУ ДЛЯ ОПЕРАТОРІВ ЗВ'ЯЗКУ 21
2.1 Системи моніторингу 21
2.2 Типи та топологія систем моніторингу 22
2.3 Архітектура систем моніторингу та механізми моніторингу 23
2.4 Порівняльні характеристики систем моніторингу 27
2.5 Системи моніторингу ЦОД 29
2.6 Висновки до розділу 2 34
РОЗДІЛ 3. ОГЛЯД ОСНОВНИХ ПРОГРАМНИХ ТА АПАРАТНИХ ЗАСОБІВ, ЩО ВИКОРИСТОВУЮТЬСЯ ПРИ СТВОРЕННІ МАКЕТА 36
3.1. Одноплатний комп`ютер - Raspberry Pi 36
3.2. Переваги одноплатних комп`ютерів 38
3.3. Система моніторингу з використанням Raspberry Pi, датчиками та протоколом ZIGBEE 38
3.4. Система моніторингу Nagios 41
3.4.1. Системи моніторингу 41
3.4.2 Огляд програми Nagios 43
3.4.3 Основні переваги та недоліки системи моніторингу Nagios 45
3.4.4 Архітектура Nagios 48
3.5 Висновки до розділу 4 51

РОЗДІЛ 4. СТВОРЕННЯ МАКЕТА РЕЛІЗАЦІЇ СИСТЕМИ МОНІТОРИНГУ ДЛЯ ЦЕНТРІВ ОБРОБКИ ДАНИХ..... 53
4.1 Необхідні елементи для створення макетів 53
4.2. Конструювання макету з центральним вузлом - Raspberry Pi 3 Model B+..... 54
4.2.1 Огляд Raspberry Pi 3 Model B+..... 54
4.2.2 Встановлення графічної бібліотеки GD 57
4.2.3 Встановлення web-серверу Apache..... 58
4.2.4 Встановлення Nagios на центральний вузол макета..... 59
4.2.5 Підключення центрального вузла та перевірка доступності вузлів мережі61
4.3 Конструювання макету з центральним вузлом - сервером HP Proliant DL120 G5 61
4.3.1 Загальні технічні характеристики серверу - HP Proliant DL120 G5. 61
4.3.2 Встановлення системи моніторингу Nagios на центральний вузол - HP PROLIANT DL120 G5 63
4.4 Система моніторингу Nagios, що реалізована на сервері в умовах проходження трафіку та процесів реального ЦОД 67
4.5 Порівняння економічних та експлуатаційних показників при різних типах реалізації системи моніторингу Nagios 71
4.5.1 Порівняння експлуатаційних показників при різних типах реалізації системи моніторингу Nagios..... 71
4.5.2 Порівняння економічних показників при різних типах реалізації системи моніторингу Nagios..... 75
4.6 Висновки до розділу 5..... 76
ВИСНОВКИ 77
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ..... 80

ПЕРЕЛІК СКОРОЧЕНЬ

GD	Graphics Library – програмна бібліотека для динамічної роботи з зображеннями
ICMP	Internet Control Message Protocol – міжмережевий протокол керуючих повідомлень
I²C/TWI	Two Wire Interface – послідовна шина даних для зв'язку інтегральних схем
IDE	Integrated Development Environment – інтегроване середовище розробки
NEB	Nagios Even Broker – модуль в Nagios
NRPE	Nagios Remote Plug-in Executor – плагін для Nagios
RAM	Random Access Memory – пам'ять з довільним доступом
SNPM	Simple Network Management Protocol – простий протокол керування мережею
SSH	Secure SHell – мережевий протокол, що дозволяє проводити віддалене управління комп'ютером і тунелювання TCP-з'єднань TCP
TCP	Transmission Control Protocol – протокол керування передачею
TCP/IP	Transmission Control Protocol – протокол керування передаванням; Internet Protocol – міжмережевий протокол. Набір протоколів мережі Інтернет
VL2	Virtual Layer 2 – тип мережевої архітектури ЦОД
VLB	Valiant Load Balancing – достовірне балансування навантаження
ДЖБ	Джерело безперебійного живлення
ОС	Операційна система
ПЗ	Програмне забезпечення
ПК	Персональний комп’ютер
ЦОД	Центр обробки даних

ВСТУП

Ріст та розвиток інформаційних ресурсів, розростання потоків даних стимулює розвиток центрів обробки даних, що в свою чергу вимагає розвиватися системи моніторингу та управління для центрів обробки даних.

Сучасні системи моніторингу центрів обробки даних мають значну надлишковість, як у обчислювальних потужностях так і у споживаних ресурсах, також такі системи є досить складними у впровадженні та експлуатації. Собівартість встановлення та експлуатації високо потужних систем моніторингу центрів обробки даних залишається високою, що, в свою чергу, знижує темпи їх розвитку, впровадженні, застосовані та оновленні в уже існуючих центрах обробки даних. Тому дуже важливим, для розвитку систем моніторингу центрів обробки даних та самих ЦОД є спрощення архітектури, зменшення споживаних ресурсів та оптимізація обчислювальних потужностей. До того ж спрощення архітектури дозволить спростити експлуатацію та впровадження даних систем моніторингу в уже існуючих центрах обробки даних. Вартість систем моніторингу також необхідно знижувати, що можливо за рахунок оптимізації їх реалізації та обчислювальних потужностей.

Об’єкт роботи: система моніторингу дата-центру.

Предмет роботи: реалізація системи моніторингу центра обробки даних з використанням одноплатних комп`ютерів для оптимізації затрат на встановлення та експлуатацію системи.

Мета роботи: реалізація системи моніторингу центра обробки даних з використанням одноплатних комп`ютерів для оптимізації затрат на встановлення та експлуатацію системи. Проведення дослідження економічних та експлуатаційних показників при різних реалізаціях системи моніторингу.

Для досягнення мети дослідження було поставлено та вирішено такі основні задачі:

1. Аналіз стану проблеми, огляд інтернет публікацій та літературний джерел.

2. Огляд центрів обробки даних та їх систем моніторингу.

3. Порівняння архітектури систем моніторингу, виділення їх основних переваг та недоліків.

4. Створення реалізації системи моніторинг для центрів обробки даних на основі одноплатних комп`ютерів.

5. Створення макету та його випробування.

6. Порівняння економічних та експлуатаційних показників при різних реалізація веб-монітору Nagios.

7. Написання загальних висновків і остаточне оформлення роботи.

Теоретичний результат дослідження:

1. Розглянуто загальні відомості про центри обробки даних та їх системи моніторингу.

2. Проведено аналіз переваг та недоліків існуючих систем моніторингу.

3. Запропоновано реалізацію системи моніторингу ЦОД на основі одноплатного комп`ютеру Raspberry Pi.

Практичний результат роботи: проведено апробацію реалізацію системи моніторингу, запропонованої у роботі, виконану з використанням макета, створеного в процесі роботи. Проведення дослідження економічних та експлуатаційних показників при різних реалізаціях системи моніторингу. Реалізоване рішення дозволяє отримувати повноцінну систему моніторингу для центрів обробки даних за менші кошти та зі спрощеною схемою обслуговування та керування.

РОЗДІЛ 1. ЗАГАЛЬНИЙ ОГЛЯД ЦЕНТРІВ ОБРОБКИ ДАНИХ ТА СИСТЕМ МОНІТОРИНГУ

1.1 Загальні відомості про ЦОД

У сучасному розумінні дата-центр, або центр обробки даних (ЦОД), – це комплексне організаційно-технічне рішення, призначене для створення високопродуктивної і відмовостійкої інформаційної інфраструктури. У більш вузькому сенсі ЦОД – це приміщення, призначене для розміщення обладнання для обробки і зберігання [1].

Залежно від призначення розрізняють три різних типи дата-центрів, кожен з яких розрахований на певну модель підприємства і має власні оперативні завдання і проблеми:

- корпоративні дата-центри;
- хостингові дата-центри, що надають комп'ютерну інфраструктуру як послугу;
- дата-центри, що використовують технологію Web 2.0.

Нижче наведені параметри, які можуть значно відрізнятися в різних типах дата-центрів:

- тип трафіку (внутрішній, зовнішній або змішаний);
- використання Layer 2 (L2) і / або Layer 3 (L3) для управлення трафіком в центрі або на периферії;
- технологія зберігання даних;
- рівень серверної віртуалізації;
- загальний розмір центру обробки даних (за кількістю серверів) [2].

1.2 Склад ЦОД

Обов'язкові компоненти, що входять до складу ЦОД, можна розділити на три основні групи:

1. Технічні компоненти. Вони створюють умови для ефективної роботи центру, до таких належать:

- серверний комплекс, включає сервери інформаційних ресурсів, додатків, подання інформації, а також службові сервери;
- система зберігання даних і резервного копіювання – ядро ЦОД. Вона складається з консолідуючих дискових масивів, мережі зберігання даних, системи резервного копіювання та аварійного відновлення даних;
- мережева інфраструктура забезпечує взаємодію між серверами, об'єднує логічні рівні і організовує канали зв'язку. Вона включає магістралі для зв'язку з операторами загального доступу, телекомунікації, що забезпечують зв'язок користувачів з ЦОД;
- інженерна система експлуатації ЦОД підтримує умови для нормального функціонування центру. До її складу входять підсистеми енергозабезпечення, кліматконтролю, пожежної сигналізації і пожежогасіння, передачі даних, а також автоматизовані системи диспетчеризації, управління інформаційними ресурсами;
- система безпеки запобігає несанкціонованому вторгненню в зони конфіденційної інформації. Вона складається з засобів захисту, системи оповіщення та системи контролю доступу.

2. Програмне забезпечення. Це фактично сервіси інфраструктури ЦОД для коректної роботи бізнес-процесів, необхідних для конкретної організації. До компонентів інфраструктури відносяться:

- операційні системи серверів;
- програмне забезпечення баз даних;
- операційні системи робочих станцій;
- засоби кластеризації;
- кошти резервного копіювання;
- програми пристроїв зберігання даних;
- засоби адміністрування серверів і робочих станцій;
- кошти інвентаризації;

- офісне програмне забезпечення;
- електронна пошта;
- Інтернет-браузери.

3. Організаційне середовище вирішує питання, пов'язані з наданням IT-послуг. Воно повинна відповідати вимогам з надання IT-послуг, таким як ISO / IEC 20000, тут представлені:

- процеси надання послуг, тобто якість і доступність послуг;
- процеси взаємин між постачальником і клієнтом, а також з підрядними організаціями;
- процеси вирішення проблем, що виникають при функціонуванні будь-якого з компонентів системи;
- процеси управління конфігураціями, моніторинг і контроль статусу IT-інфраструктури, інвентаризація, верифікація та реєстрація конфігураційних одиниць, збір і управління документацією, надання інформації про IT-інфраструктурі для всіх інших процесів;
- процеси управління змінами, тобто визначення необхідних змін і способів їх проведення з найменшим ризиком для IT-послуг, а також проведення консультацій та координації дій з організацією в цілому;
- процеси релізу, тобто спільного тестування і введення в активну діяльність організації ряду конфігураційних одиниць.[3]

1.3 Топологія ЦОД

Мережа центрів обробки даних побудована для кращого розміщення динамічних віртуалізованих серверів та середовищ зберігання, тоді як архітектура Дата-центр мережі розглядається як один з найважливіших факторів, що визначають продуктивність мережі, і вона відіграє значну роль у задоволенні вимог служб мікроконтролерів, а також оперативності і динамічної спроможності інфраструктури змінювати вимоги до програм.

Як правило, топології ЦОД можна грубо класифікувати за чотирма категоріями:

- топологія на основі дерев (наприклад, Fat-Tree, VL2, Portland);
- рекурсивна топологія (наприклад, DCell, BCube, FiConn, FlatNet, SprintNet);
- гібридна мережа (наприклад, c-Through, Helios);
- пряма мережа (наприклад, CamCube, Small-World).

Якщо розглядати питання, чи змінюється топологія мережі з моменту її розгортання, топології ЦОД можна розділити на фіксовану топологію (наприклад, Fat-Tree, Portland, VL2, DCell, BCube та ін.) та подвижну топологію (наприклад, c-Through, OSA, Helios).

Деякі основні топології на основі дерева (більшість ЦОД в Україні побудовані по даній топології) :

- Основне дерево. Традиційна топологія базових деревних мереж, показана на рисунку 1.1, зазвичай будується з двох або трьох рівнів, які мають рівень доступу, рівень агрегації (при необхідності) та рівень ядра. Сервери - це листя дерев, які з'єднуються з багатьма перемикачами верхніх стійок. Ці перемикачі верхніх стійок потім взаємопов'язані через кінцеві стійки, які в свою чергу підключаються через сердечники. Рівень агрегації забезпечує обслуговування домену та балансування навантаження, тоді як рівень ядра взаємопоєднує об'єкти агрегації та керує трафіком у центрі обробки даних та його виведенням.

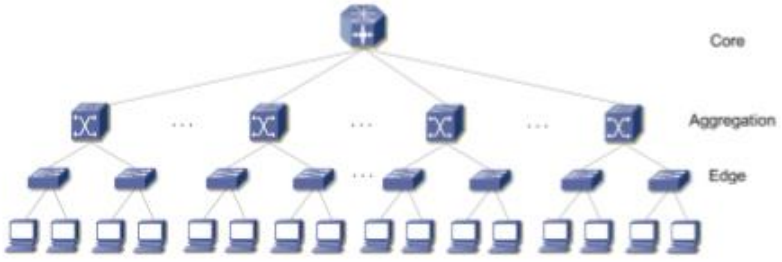

Рисунок 1.1 Традиційна 3-рівнева деревоподібна мережева топологія

- FAT-TREE. На рисунку 1.2 представлена топологія Fat-Tree, яка складається з Clos-мережі, побудованої у формі багатокористувацького дерева. Згодом Fat-Tree використовувалася як типова топологія для дослідження дослідницької мережі центрів обробки даних, наприклад, Portland, Hedra, Elastic Tree тощо.

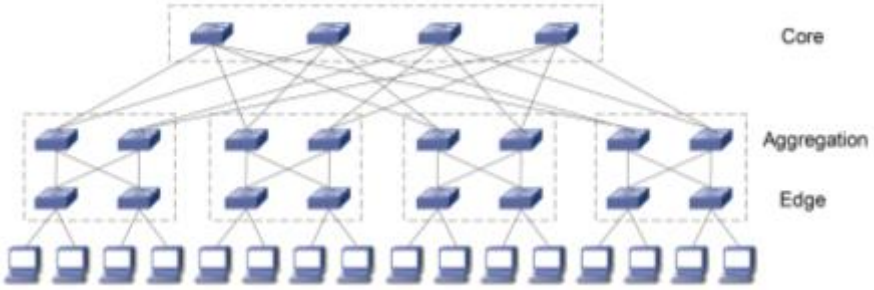

Рисунок 1.2 Проста 3-рівнева топологія Fat-Tree

- VL2 [4] - це гнучка та економічно ефективна мережева архітектура, яка побудована з численних перемикачів, розташованих у топології Clos. VL2 використовує достовірне балансування навантаження (VLB) для поширення трафіку через мережеві шляхи та використовує рішення для підтримки великих серверних пулів. Крім того, VL2 застосовується для усунення фрагментації ресурсів і дозволяє будь-яку службу призначити будь-якому серверу в будь-якому місці ЦОД. Тим не менш, система може бути неефективною у випадку великого завантаження мережі.
- DCell [5], як показано на рисунку 1.3, використовує сервери з декількома портами та міні-комутаторами нижчого рівня для побудови рекурсивно-дефіцитної архітектури. InDCell, що має назву DCell0, складається з n серверів та одного перемикача n-port . Кожен сервер у DCell0 підключається до перемикача в тому ж DCell0. Тим не менше, якщо посилання на нижньому рівні несуть більше трафіку то це призведе до використання вищої лінії зв'язку, що призводить до низької пропускної спроможності вузлів.

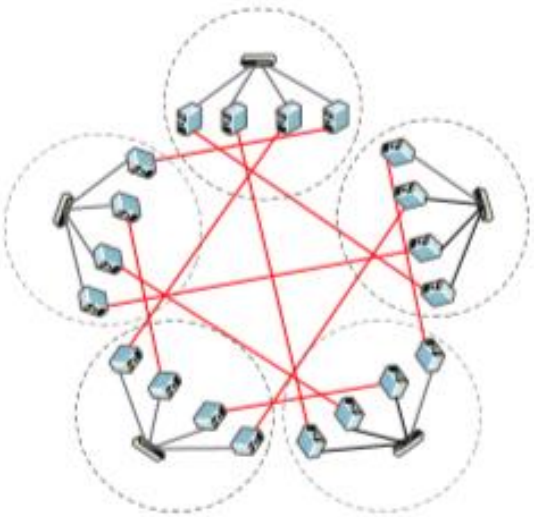

Рисунок 1.3 Приклад топології DCell

1.4 Основні недоліки ЦОД

Серед недоліків ЦОД виділимо наступні:

- складна архітектура, високий відсоток відмов;
- складне обслуговування і керування;
- недостатність ресурсів віртуалізації ;
- недостатність ресурсів, неефективне використання кросування;
- значні потреби в продуктивності та ємності.

Дата-центр являє собою сукупність спланованих певним чином територій, зовнішніх майданчиків, будівель, приміщень, зі встановленими інженерними системами забезпечення та обслуговуючим персоналом, що утворюють загальний фізичний простір і технологічне середовище для розміщення комп'ютерів, електронних та інших засобів прийому, передачі, обробки, зберігання інформації і забезпечують задану ступінь доступності (готовності), розміщеного обладнання в заданому режимі функціонування[11]. Будівництво та експлуатація центрів обробки даних здійснюється згідно з рядом жорстких стандартів, що й становить складне обслуговування і керування, а також складну архітектуру і пов`язаний з цим високий відсоток відмов.

Мале використання системи віртуалізації призводить до ускладнення схем кросування, заплутаності архітектури. Окремі кабелі для зберігання та керування мережами, призводять до складних кабельних з`єднань і зниження утилізації кабелів, підвищення вимог до пожежної безпеки.

1.5 Висновки до розділу 1

У даному розділі було розглянуто та проаналізовано інформацію про ЦОД:

1.Розгляд загальних відомостей про центри обробки даних.

2.Розглянуто складові центрів обробки даних.

3.Розглянуто основні топології побудови ЦОД.

4.Перечислено основні недоліки ЦОД.

Центр обробки даних (ЦОД), – це комплексне організаційно-технічне рішення, призначене для створення високопродуктивної і відмовостійкої інформаційної інфраструктури.

Обов'язкові компоненти, що входять до складу ЦОД, можна розділити на три основні групи: технічні компоненти, програмне забезпечення, організаційне середовище.

Топології ЦОД можна грубо класифікувати за чотирма категоріями: топологія на основі дерев (наприклад, Fat-Tree, VL2, Portland); рекурсивна топологія (наприклад, DCell, BCube, FiConn, FlatNet, SprintNet); гібридна мережа (наприклад, c-Through, Helios); пряма мережа (наприклад, CamCube, Small-World).

Серед основних недоліків ЦОД виділяються наступні: складна архітектура, високий відсоток відмов; складне обслуговування і керування; недостатність ресурсів віртуалізації; недостатність ресурсів, неефективне використання кросування; значні потреби в продуктивності та ємності.

РОЗДІЛ 2. РОЗГЛЯД СИСТЕМ МОНІТОРИНГУ ДЛЯ ОПЕРАТОРІВ ЗВ'ЯЗКУ

2.1 Системи моніторингу

Система моніторингу – група пристроїв та програмне забезпечення, що забезпечує систематичний збір і обробку інформації, яка може бути використана для поліпшення процесу прийняття рішення, а також, побічно, для інформування громадськості або прямо як інструмент зворотного зв'язку з метою здійснення проектів, оцінки програм або вироблення політики. Вона несе одну або більше з трьох організаційних функцій:

- виявляє стан критичних або знаходяться в стані зміни явищ навколишнього середовища, щодо яких буде вироблений курс дій на майбутнє;
- встановлює відносини зі своїм оточенням, забезпечуючи зворотний зв'язок, щодо попередніх успіхів і невдач певної політики або програм;
- встановлює відповідності правилам і контрактним зобов'язанням.

Засоби контролю (моніторингу) дозволяють стежити за процесами, що відбуваються в системі. При цьому можливі два підходи: спостереження в реальному режимі часу або контроль з записом результатів у спеціальному протокольному файлі. Перший підхід зазвичай використовують при вишукуванні шляхів для оптимізації роботи обчислювальної системи та підвищення її ефективності. Другий підхід використовують, коли моніторинг виконується автоматично і (або) дистанційно, про останньому випадку результати моніторингу можна передати віддаленої службі технічної підтримки для встановлення причин конфліктів в роботі програмного і апаратного забезпечення [6].

Моніторинг інженерної інфраструктури ведеться по трьом напрямкам:

1. По автономним датчикам (протікання, температурні, руху і т.п.):

- датчики протікання потрібні завжди, особливо якщо в дата-центрі використовується система охолодження з рідким теплоносієм або фреонова зі зволоженням;
- температурні датчики встановлюємо в холодних і гарячих коридорах машинних залів, в приміщеннях з інженерною інфраструктурою;
- датчики руху, відкриття і закриття дверей стійок.

2. Моніторинг обладнання (кондиціонери, ДБЖ, камери та ін.):

- чи працює обладнання в штатному режимі;
- які помилки виникають в роботі;
- значення окремих параметрів (напруга в ДБЖ, сила струму, температура на вході і виході кондиціонерів та ін.).

3. Моніторинг системи в цілому.

2.2 Типи та топологія систем моніторингу

Система моніторингу може бути визначена як елемент, який реалізується в мережі. Система моніторингу періодично перевіряє доступність і стан кожного вузла і елемента мережі. У разі якщо є якісь проблеми або якщо деякі елементи недоступні то про це автоматично повідомляється відповідальній особі. У деяких випадках можливо активно управляти мережею за допомогою системи моніторингу. Також можливо визначити способи, які будуть використовуватися у випадку якщо критичний вузол недоступний, але це залежить від типу системи моніторингу - в цілому їх можна розділити на три типи. Можуть використовуватися системи моніторингу як додаток на сервері (випадок порівнюваних систем) або як індивідуальний пристрій.

Виділимо наступні типи систем моніторингу:

1. Базові системи моніторингу.

Базові системи моніторингу зазвичай працюють з протоколом ICMP. Ці системи періодично перевіряють тільки стан елементів, і вони можуть надавати інформацію про його доступності тільки на доступному / недоступному рівні або вони додають інформацію про час відповіді. Цей тип системи моніторингу підходить тільки для невеликих локальних мереж або для мереж, які не можуть надати більше інформації.

2. Розширені системи моніторингу.

Цей тип моніторингу зазвичай працює з великою кількістю протоколів таких як SNMP, CDP, SSH і так далі. Цей факт дозволяє системам моніторити практично всю інформацію про пристрої в мережі як стан запущених служб, використання системних ресурсів, фактичний потік даних і так далі. З серверами ці системи зазвичай використовують локальні оператори.

3. Системи моніторингу з активним контролем.

Системи моніторингу з активним контролем більш-менш розвинені і може керувати мережевими пристроями. Ці системи дозволяють адміністратору реалізувати автоматичний сценарій, який реагує на зумовлені події і підходять для центрів обробки даних, великих мереж, високодоступних кластерів і так далі.

2.3 Архітектура систем моніторингу та механізми моніторингу

Незважаючи на те, що кожна мережа даних по суті унікальна існує загальна ідея, яка широко застосовується в мережі передачі даних. Архітектури щодо надійності, швидкості і надійності передачі даних. Цю архітектуру найкраще характеризує і описує компанія Cisco і її Enterprise Campus 3,0 [7]. Принцип цієї архітектури – трирівнева ієрархічна мережа з ядром, розподілом і рівнями доступу, яка дозволяє і полегшує майбутнє зростання мереж і значно полегшує маршрутизацію,

адресацію і автономію окремих компонентів і блоків мережі. З точки зору систем моніторингу, одним з найбільш фундаментальних питань є питання їхнього розташування в контрольованої мережі. На думку автора, логічним місцем для його розташування є основний шар, який повинен забезпечити максимальну доступність і в той же час система моніторингу - доступ до всіх шарів елементів мережі.

Коли ви використовуєте систему моніторингу, ви повинні розуміти розмір контрольованої мережі і відповідно до неї повинні вибрати відповідну цьому архітектуру. Взагалі кажучи, на даний час ми використовуємо дві системи систем моніторингу - централізований і об'єднаний.

1. Централізована система моніторингу.

Основна архітектура та впровадження системи моніторингу підходять для невеликих мереж без зовнішніх галузей. Система моніторингу використовується там лише з одним сервером, який контролює всю мережу. Якщо необхідно також контролювати зовнішню гілку, у більшості випадків використовується VPN-сайт. Якщо використовується ця архітектура, надзвичайно важливо вибрати відповідне місце системи моніторингу. Логічно, що найкраще місце для його з'єднання в центрі мережі (ядро мережі).

Перевагою цієї архітектури є простота та швидкість реалізації. Найбільш ризикованою і найбільш складною точкою її реалізації є чітко визначена концепція системи моніторингу. Архітектура з централізованою системою моніторингу зображена на рисунку 2.1.

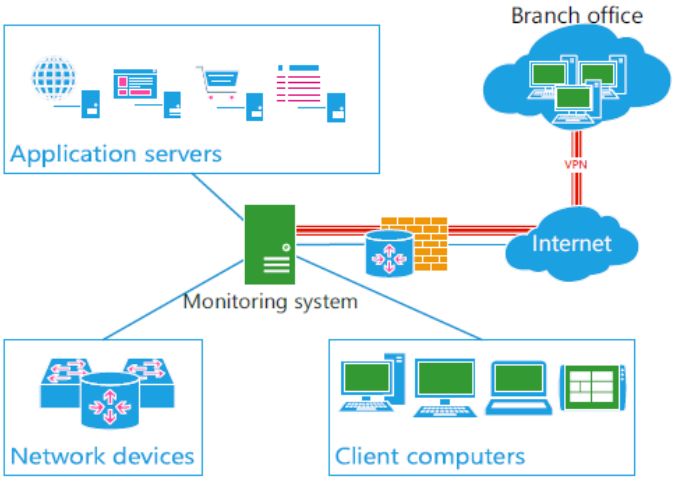

Рисунок 2.1 Архітектура з централізованою системою моніторингу

2. Система федеративного моніторингу.

Ця архітектура базується на сегментації відстежуваної мережі до менших частин, які контролюються індивідуальною системою моніторингу. Ці менші сервери повідомляють повну інформацію про мережу з їх точки зору на центральний сервер моніторингу. Центральний моніторинг на основі інформації від галузевих систем може точно звітувати про постраждалий сегмент мережі. У разі виходу з ладу основної системи моніторингу все ще можливо отримати дані та інформацію від галузевих систем. Цей тип архітектури підходить особливо для розгалужених мереж, або, з іншого боку, для постачальників, які можуть використовувати його для спостереження за своїми клієнтами мереж та виходів з основної системи моніторингу, а потім представляти їх в центр моніторингу. Архітектура з федеративною системою моніторингу зображена на рисунку 2.2.

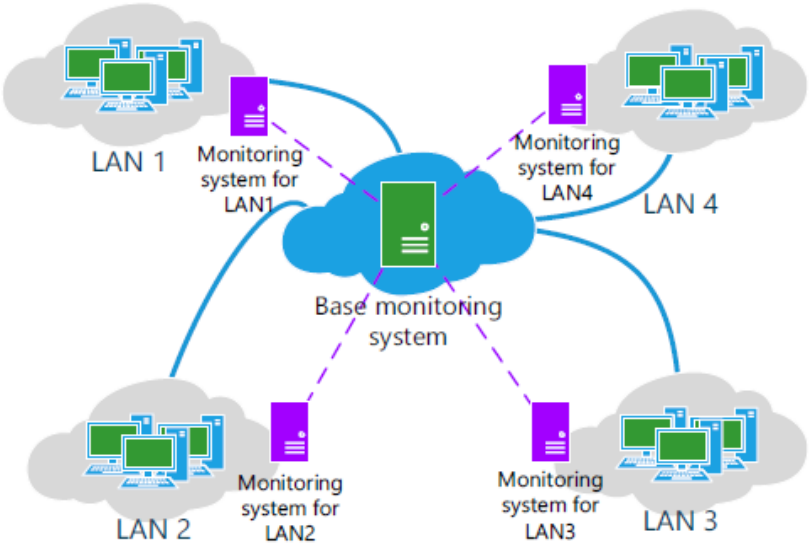

Рисунок 2.2 Архітектура з федеративною системою моніторингу

Системи моніторингу для збору інформації з контрольованих пристроїв використовують три методи. Перший метод перевіряє пристроїв з використанням стандартних протоколів, таких як ICMP, TCP, SNMP і так далі. Такий спосіб перевірки в більшості випадків не потребує будь-якого великого втручання до конфігурації за винятком дозволу виключень в брандмауері. Це також універсальний метод отримання інформації незалежно від виробників та типу пристрою. Недоліком є певне узагальнення та недоступність деяких спеціалізованих функцій.

Другий варіант - використання SNMP-повідомлення під назвою SNMP пастка. На противагу першому варіанту немає періодичної перевірки з боку системи моніторингу, але контрольований елемент в випадку аварії (помилка, збій порту, RAM заповнений, і так далі) відправить звіт в систему моніторингу, на основі отриманої інформації. Цей спосіб перевірки у більшості випадків поєднуються з періодичної перевіркою [8].

Третій варіант, як отримати дані системи моніторингу, - використання спеціального агента для моніторингу пристрою. Агент працює в цільовій системі як додаток, і він взаємодіє з системою моніторингу за принципом клієнт-сервер. Перевага в тому, що ви не повинні використовувати спеціальний

мережевий протокол, оскільки ці дані переважно передаються через TCP/IP. Головною перевагою є можливість отримати детальну інформацію про моніторингову систему, а в разі активної системи моніторингу також є можливість керувати станцією, що підлягає моніторингу. Сервери зазвичай контролюються таким способом.

2.4 Порівняльні характеристики систем моніторингу

Якщо ви хочете об'єктивно протестувати та порівняти обрані системи моніторингу, необхідно встановити критерії оцінки та методи оцінки даних. У реальному застосуванні, весь процес повинен складатися з кількох етапів: визначення вимог, дослідження ринку для потенційно придатних систем, застосування методології, реалізація переможця.

Виділимо наступні критерії оцінки:

- Ціна

У той момент, коли ми будемо приймати рішення про те, яка система моніторингу повинна бути використана, її ціна завжди буде одним із найважливіших критеріїв. На жаль, ціна занадто завищена, і переважна більшість компаній не зможе правильно аналізувати цей параметр. Ціну слід завжди аналізувати пропорційно до того, що система принесе нам, і де це дозволить заощадити нашу трудомісткість або оптимізувати процеси.

- Системні вимоги

Критерій, який оцінює мінімальні вимоги до запуску системи як з точки зору навантаження, так і додаткових програм.

- Користувацький інтерфейс

Ймовірно, найменший предикативний критерій. В основному це пов'язано з тим, що інтерфейс вигляду та роботи з користувачами настільки суб'єктивний, що практично неможливо отримати об'єктивну оцінку.

- Труднощі виконання

Критерій оцінки складності установки та базової конфігурації системи моніторингу.

- Швидкість відповіді на аварію

Критерій, який оцінює здатність системи реагувати на провал будь-якого елемента в мережі.

- Можливість ідентифікації постраждалого сегмента

Оцінка особливо з точки зору можливості визначити ієрархію моніторингової мережі та наслідком здатність виявляти уражений сегмент у разі невдачі.

- Автоматичний пошук

Функція, яка автоматично сканує область моніторингу та виконує пошук вузлів мережі для відстеження. Системи моніторингу для цього відстеження використовують протоколи ICMP та SNMP. Деякі системи потім використовують також утиліту traceroute для виявлення шляху передачі знайдених вузлів. З точки зору цього критерію оцінюється, зокрема, якість сканування, швидкість і визнання фактичної топології мережі.

- Методи повідомлення

Оцінка з точки зору інформації про ситуацію в мережі надсилається адміністратору. Коли ми забиваємо кожну точку, надану системі, це наявна технологія. Системні типи віддають перевагу електронній пошті або SMS. Деякі з них також додають підтримку різних мереж зв'язку, таких як Jabber і так далі.

- Додаткові функції

Критерій оцінки додаткових функцій, які не є частиною стандарту, на всіх випробуваних системах моніторингу.

- Співпраця з іншими системами

Це вивчення сумісності між системами моніторингу та методом, якщо такі існують, як можна підключити системи або як їх об'єднати.

- Глибина моніторингу

Вона оцінює вивчену систему з точки зору наявної інформації про пристрої, що підлягають моніторингу.

2.5 Системи моніторингу ЦОД

Система моніторингу – група пристроїв та програмне забезпечення, що забезпечує систематичний збір і обробку інформації, яка може бути використана для поліпшення процесу прийняття рішення, а також, побічно, для інформування громадськості або прямо як інструмент зворотного зв'язку з метою здійснення проектів, оцінки програм або вироблення політики[3].

Сучасні системи моніторингу для ЦОД умовно можна розділити на дві великі групи, як зображено на рисунку 2.1:

- контроль параметрів зовнішнього середовища;
- контроль стану інфраструктурного обладнання.

Головними структурними елементами систем обох груп є різноманітні датчики та контролери показники яких й передаються на центральну систему моніторингу, а також спеціалізоване ПЗ для управління та налаштування.

Як правило компанії, котрі виробляють одночасно ДБЖ, системи кондиціонування, розподіл електроживлення, а також інші елементи інженерних підсистем ЦОД, пропонують своїм замовникам комплексні рішення. Найвідоміші виробники продукції такого плану, які представлені у нашій країні - APC, Conteg, Eaton, Knurr, Rittal, Vutlan.

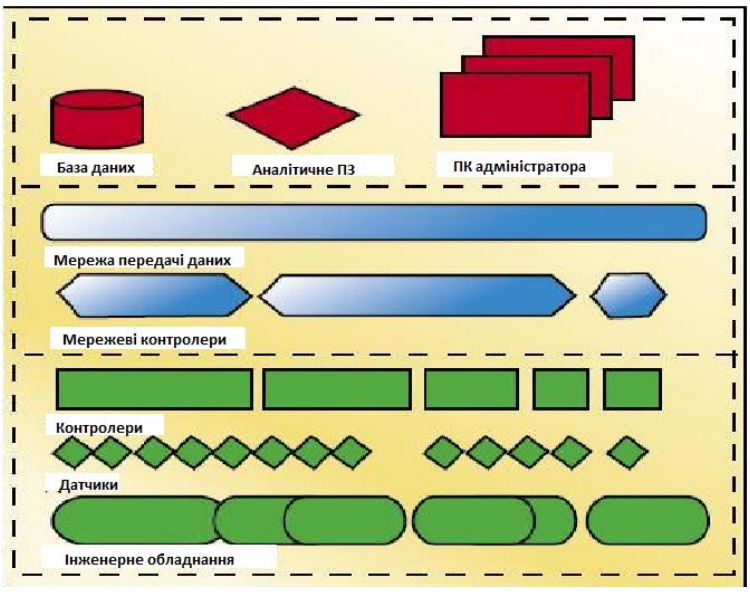

Рис. 2.3 Архітектура систем моніторингу інженерної інфраструктури і параметрів зовнішнього середовища ЦОД

Найчастіше модуль моніторингу використовується в IT сфері для моніторингу параметрів ЦОД: температури, вологості, стану обладнання, параметрів електроживлення, наявності підтікання та відсутності загоряння. Іноді зустрічаються нестандартні рішення використання систем моніторингу для відстеження параметрів обладнання: кондиціонерів, шаф, верстатів, об'єктів телематики, розумного будинку. Порівняємо дві системи моніторингу параметрів APC NetBotz 200 і Vutlan SC8100.

Порівняння проведемо по 3 категоріям:

- технічні характеристики і можливість масштабування / розширення;
- можливості системи;
- ціна.

У першому випадку, розглянемо основні відмінності в характеристиках. Порівнювати будемо тільки ті параметри, відмінності в яких впливають на зручність монтажу або експлуатації системи. У цьому ж пункті розглянемо можливість масштабування системи: кількість портів під датчики в обох системах моніторингу, відмінності і різноманітність датчиків. У другому

випадку, розглянемо програмні можливості систем моніторингу параметрів. Зібрати інформацію з датчиків - це третина завдання. Головне оповістити обслуговуючий персонал при виході параметрів за межі норми, а в ідеалі - передбачити динаміку зміни параметрів, і не допустити виходу параметрів за межі норми. У третьому випадку порівняємо ціни на типовий набір модулів і датчиків систем моніторингу.

1. Технічні характеристики. Далі наведена порівняльна характеристика технічних параметрів для двох систем моніторингу, для наглядності – Таблиця 2.1.

Таблиця 2.1 Порівняльна характеристика технічних параметрів

Порівнювальна характеристика	Vutlan SC8100	APC NetBotz 200
Живлення	AC 220 В, DC 12 В	AC 220 В. Розетка C13 и C14
Необхідна потужність, Вт	18	51
Максимальна кількість датчиків	8	6
Максимальна кількість датчиків (з урахуванням модуля розширення)	100	
Датчик температури	Так	Так
Датчик вологості	Так	Ні
Датчик протічки	Так	Так
Датчик повітряного потоку	Так	Ні

Продовження Таблиці 2.1 Порівняльна характеристика технічних параметрів

Датчик диму	Так	Ні
Датчик струму, до 100А	Так	Ні
GSM модуль	Так, модулем	Ні
SNMP	v1+v2 або v3, є SNMP Trap	v1 або v3, є SNMP Trap
Відслідковування обладнання по ICMP	Так	Ні
Наявність NMS в Web інтерфейсі	Можливість побудови і аналіз графіків, графічні карти	Можливість побудов графіків, повідомлення про перевищення порогового значення

2. Можливості системи

І один і другий модуль системи моніторингу виконують свою основну функцію: агрегація показників датчиків, і відображення значень по Web протоколу. Даний вивід системи моніторингу показано на рисунку 2.4.

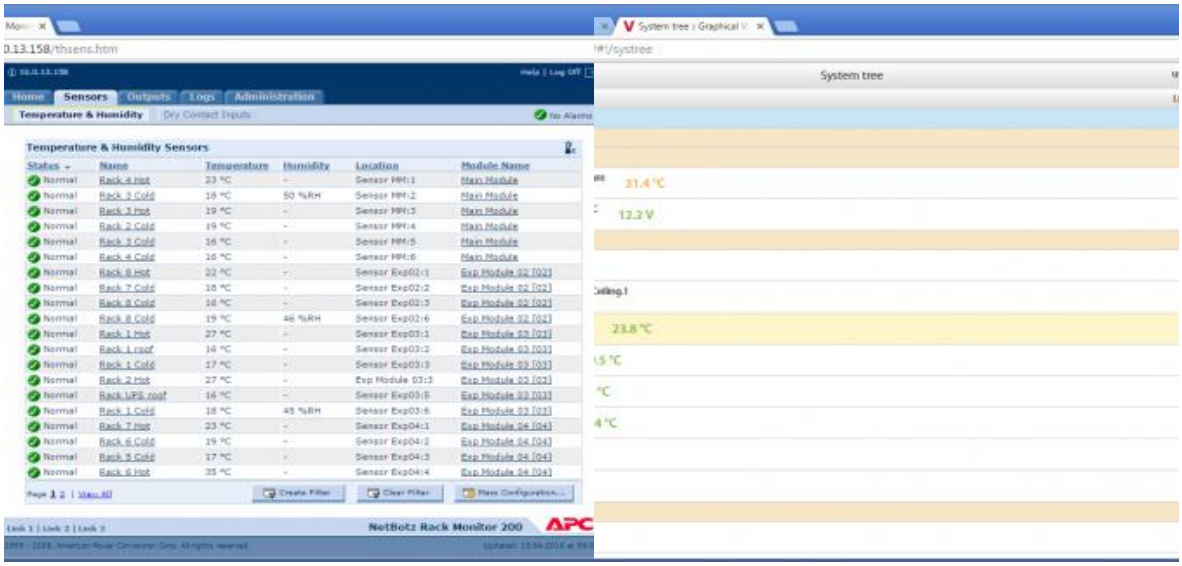

Рисунок 2.4 Відображення значень моніторингу по Web-протоколу

І в одному, і в другому модулі присутня можливість встановлювати межі значень, і повідомлення про вихід значень за межі норми. Даний вивід системи моніторингу показано на рисунку 2.5.

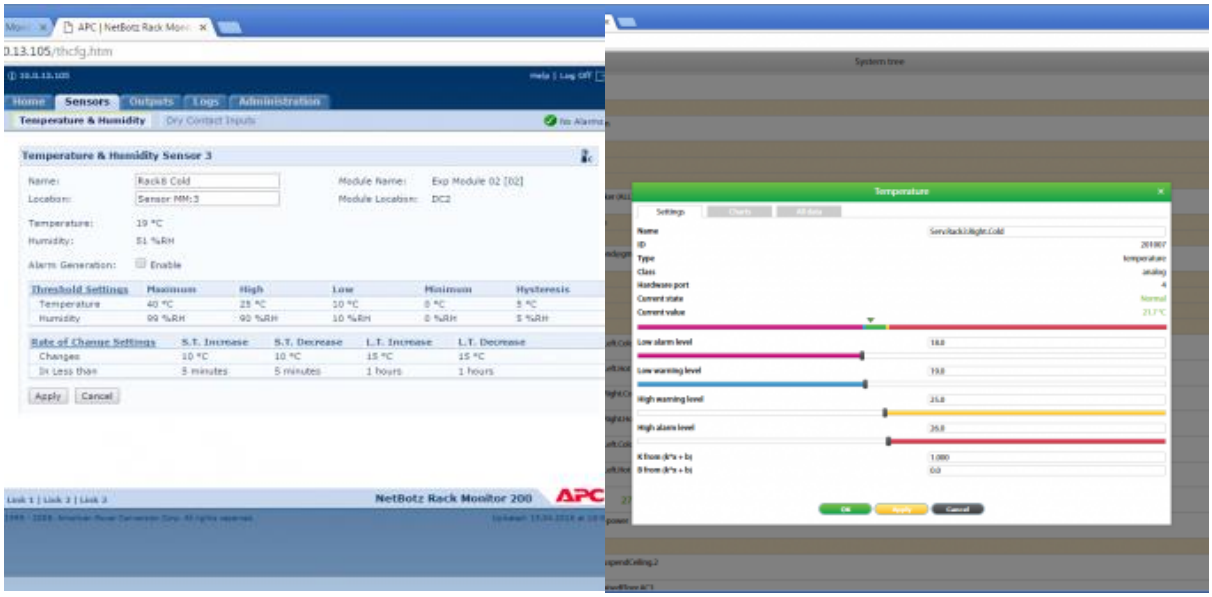

Рисунок 2.5 Відображення значень моніторингу при виході показників за межу норми

Всі додаткові, не основні функції присутні в обох системах моніторингу: ftp backup, RADUIS авторизація, ntp клієнт, syslog клієнт, графіки датчиків, як можна побачити на рисунку 2.6 [9-10].

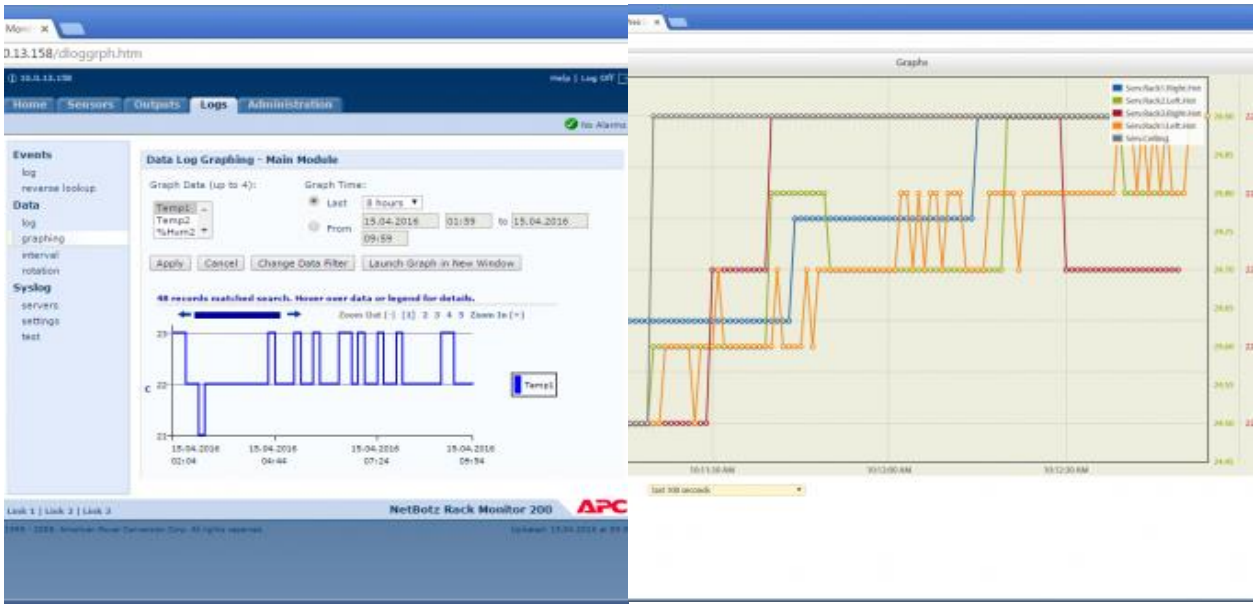

Рисунок 2.6 Відображення значень моніторингу з додатковими можливостями

3. Ціна. Далі наведена порівняльна характеристика цін для двох систем моніторингу, для наглядності – таблиця 2.2.

Таблиця 2.2 Порівняльна характеристика ціни

	Vutlan C8100	APC NetBotz 200
Модуль моніторинга Vutlan SC8100, 8 портів і APC NetBotz Rack Monitor 200, 6 портів.	$490	$377
Датчик температури	$21	$78
Датчик вологості	$38	
Датчик протічки	$32	
Датчик протічки	$32	$120
Датчик повітряного потоку	$21	
Датчик диму	$41	$170
Датчик струму, до 100 А	$48	$530

2.6 Висновки до розділу 2

У даному розділі було досягнуто наступних пунктів:

1. Розглянуто поняття – система моніторингу.
2. Приведено типи, топологію, архітектуру систем моніторингу.
3. Наведено порівняльні характеристики систем моніторингу та наведено порівняльну характеристику двох систем моніторингу.

Система моніторингу – група пристроїв та програмне забезпечення, що забезпечує систематичний збір і обробку інформації, яка може бути використана для поліпшення процесу прийняття рішення, а також, побічно, для інформування громадськості або прямо як інструмент зворотного зв'язку з метою здійснення проектів, оцінки програм або вироблення політики.

Основні функції систем моніторингу:

- виявляє стан критичних або знаходяться в стані зміни явищ навколишнього середовища, щодо яких буде вироблений курс дій на майбутнє;
- встановлює відносини зі своїм оточенням, забезпечуючи зворотний зв'язок, щодо попередніх успіхів і невдач певної політики або програм;
- встановлює відповідності правилам і контрактним зобов'язанням.

В ході роботи було виділено наступні критерії оцінки системи моніторингу:

- технічні характеристики і можливість масштабування та розширення;
- можливості системи;
- ціна.

РОЗДІЛ 3. ОГЛЯД ОСНОВНИХ ПРОГРАМНИХ ТА АПАРАТНИХ ЗАСОБІВ, ЩО ВИКОРИСТОВУЮТЬСЯ ПРИ СТВОРЕННІ МАКЕТА

У якості основних елементів системи планується використовувати комп’ютер Raspberry Pi 3 Model B+, сервер HP Proliant DL120 G5, операційна системи сімейства Linux (Raspbian, Ubuntu), у якості моніторингової системи - Nagios.

3.1. Одноплатний комп`ютер - Raspberry Pi

Raspberry Pi - це мініатюрна, і зручна платформа швидкої розробки електронних пристроїв для новачків і професіоналів, розміром з кредитну карту, ультра дешевий комп'ютер, створений Девідом Брабеном. Платформа користується величезною популярністю в усьому світі завдяки зручності, простоті і різноманіттю мов програмування, а також відкритій архітектурі і програмному коду. Пристрій програмується через USB або, безпосередньо, з середовища розробки на самому пристрої.

Raspberry Pi дозволяє комп'ютеру вийти за рамки віртуального світу у фізичний і взаємодіяти з ним. Пристрої на базі Raspberry Pi можуть отримувати інформацію про довкілля за допомогою різних датчиків, а також можуть керувати різними виконавчими пристроями.

Raspberry Pi заснований на процесорі з архітектурою ARM 11, частотою 700 МГц. В останніх версіях прошивки офіційно дозволили розганяти процесор до 1000 МГц. Це дозволяє досягти прийнятної продуктивності при низькому енергоспоживанні.

Ще однією перевагою даного мікрокомп’ютера є його, порівняно, невисока вартість на рівні близько 25-35$. У сукупності з низькими вимогами відкритого програмного забезпечення до апаратної частини і спеціально зібраним ядром операційної системи, оптимізованим під комп’ютер, це дозволяє встановити на нього операційну систему Linux (або RiscOS), а також

набір супутнього програмного забезпечення. Наприклад в тому варіанті, який передбачається зараз, там буде встановлена операційна система Debian Linux, під назвою Raspbian, браузер Midori, Все це програмне забезпечення безкоштовне, і мало вимогливо до ресурсів.

За допомогою даної платформи можливо зробити ребаланс доступної пам'яті.

Однією з важливих переваг цієї платформи, є споживана потужність Paspberry Pi - всього 1 Вт, в той час, як у традиційного системного блоку - мінімум 250 Вт.

Загальний вигляд плати Raspberry Pi зображено на рисунку 3.1.

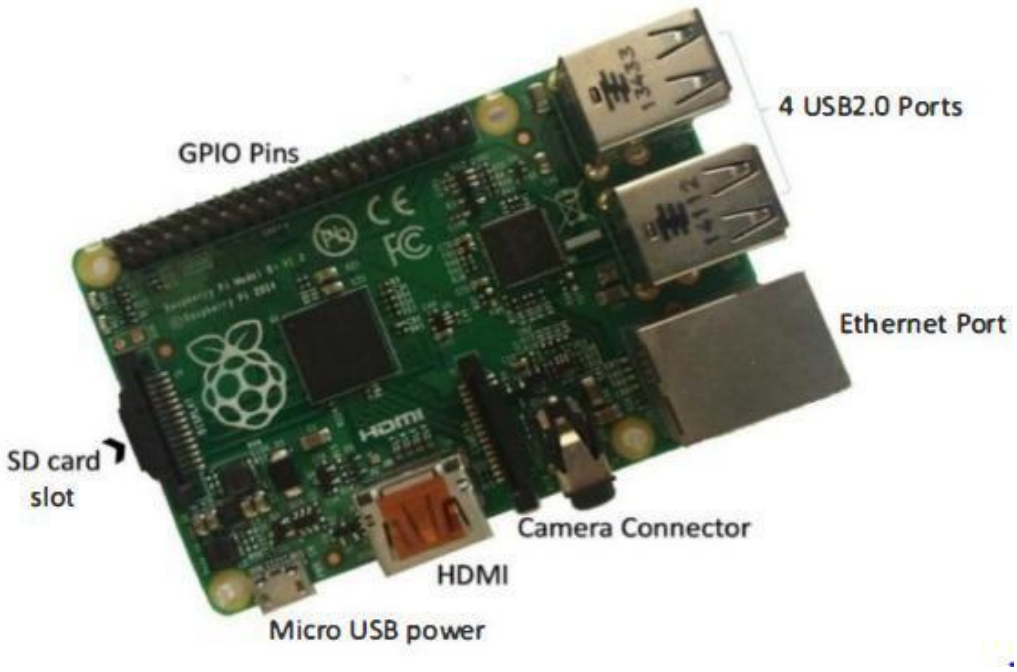

Рисунок 3.1 Загальний вигляд плати Raspberry Pi 2

Відкрите програмне забезпечення: ОС Raspbian (Debian, скомпільований під архітектуру ARM), веб-браузер Midori, встановлений інтерпретатор Python [13].

3.2. Переваги одноплатних комп`ютерів

Одноплатний комп'ютер (Single-board computer) - самодостатній комп'ютер, зібраний на одній друкованій платі, на якій встановлені мікропроцесор, оперативна пам'ять, системи введення-виведення і інші модулі, необхідні для функціонування комп'ютера. Одноплатні комп'ютери виготовляються в якості демонстраційних систем, систем для розробників або освіти, або для використання в ролі промислових або вбудованих комп'ютерів.

Кількість завдань, з якими впорається такий комп'ютер, досить велике. Список починається домашнім комп'ютером і закінчується роутерами і модемами. Наприклад, на такий пристрій можна без проблем встановити майже повний Linux, перетворивши його в механізм для роботи з документами, веб-серфінгу, прослуховування музики та інших нескладних завдань. Деякі моделі здатні підтримувати навіть програвання відеороликів аж до 1080p. І все це - зі звичним графічним інтерфейсом. Єдине місце, де можуть виникнути проблеми, - це інша архітектура. Як правильно, багато програм мають версію для ARM-архітектури, а якщо немає - легко знайти аналог, але специфічний софт на цій платформі все ще трапляється рідко.

Основними перевагами одноплатних комп’ютерів є:

- Висока продуктивність.
- Малі габарити.
- Низька собівартість.
- Простота налаштування.
- Можливість використання великого числа додаткових модулів.

3.3. Система моніторингу з використанням Raspberry Pi, датчиками та протоколом ZIGBEE

Сучасні системи моніторингу, що використовують одноплатні комп’ютери в якості базових вузлів, використовують протокол ZigBee. Кожен

сенсор мережі під'єднується до мікроконтролера, що підключається до модуля зв'язку XBee. Центральний вузол системи - це одноплатний комп'ютер, обладнаний аналогічним модулем. Живлення кожного вузла відбувається за рахунок акумулятора. На центральному вузлі встановлюється Веб-додаток, головним завданням якого є обробка даних , отриманих від вузлів з сенсорами та представлення даних кінцевому користувачеві.

Протокол ZigBee передбачає наявність головного вузла, що управляє топологією мережі, його функції бере на себе одноплатний комп'ютер.

Архітектура мережі зображена на рисунку 3.2.

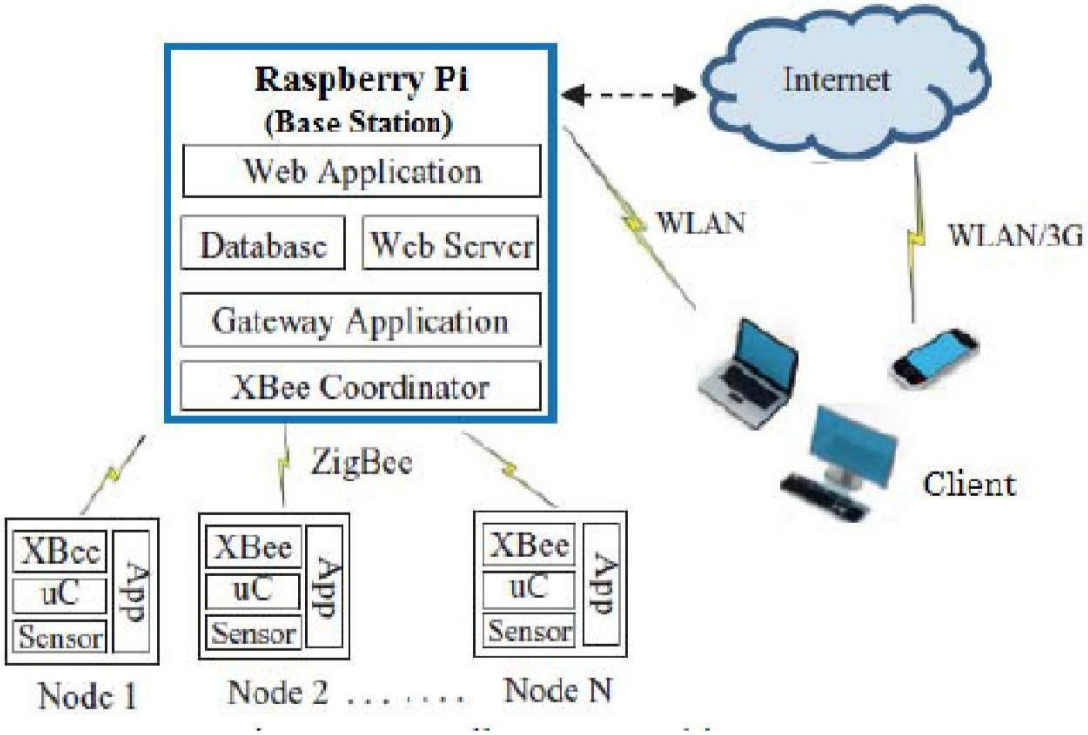

Рисунок 3.2 Архітектура системи моніторингу на основі одноплатних комп'ютерів

У якості дочірніх вузлів мережі використовуються мікроконтролери компанії Arduino - торгова марка апаратно-програмних засобів для побудови простих систем автоматики і робототехніки, орієнтована на непрофесійних користувачів. Програмна частина складається з безкоштовної програмної оболонки (IDE) для написання програм, їх компіляції та програмування апаратури. Апаратна частина являє собою набір змонтованих друкованих плат,

що продаються як офіційним виробником, так і сторонніми виробниками[12]. Повністю відкрита архітектура системи дозволяє вільно копіювати або доповнювати лінійку продукції Arduino. Блок схема центрального і дочірнього вузлів системи зображена на рисунку 3.3.

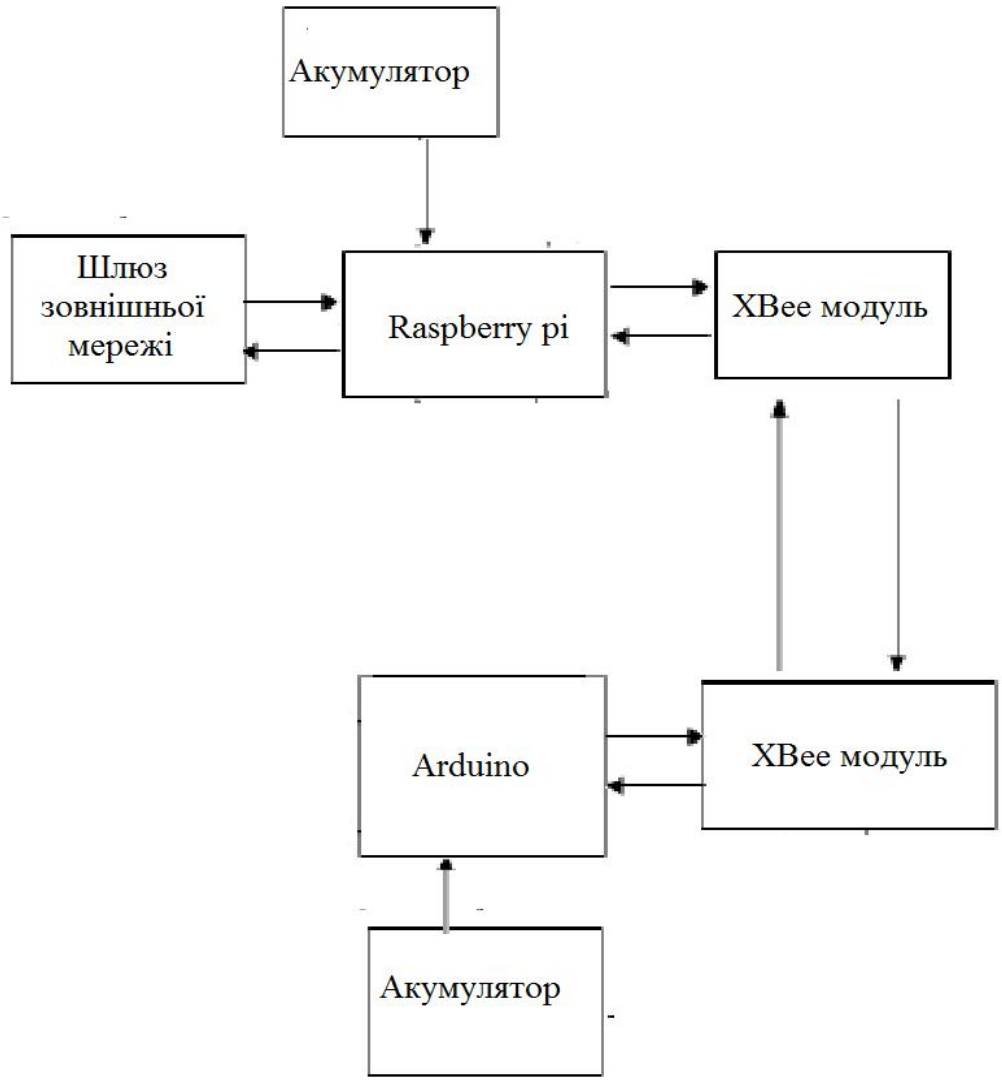

Рис. 3.3 Блок-схема центрального і дочірнього вузлів системи

Переваги:

- низькі енергетичні затрати;
- попередня обробка даних;
- можливість використання різних мереж передачі даних до кінцевого користувача;

- простота зміни конфігурацій топології системи;
- низька вартість системи.

Недоліки:

- низька швидкість передачі даних;
- необхідність періодичної заміни акумуляторів;
- необхідність використання додаткового обладнання (модулі XBee).

3.4. Система моніторингу Nagios

3.4.1. Системи моніторингу

Зовнішні пристрої, підключені до мережі, повинні регулярно відслідковуватися в режимі реального часу. Моніторинг мережі використовується для збирання даних, забезпечення статистики в режимі реального часу та аналізу ефективності роботи мережі. Якщо в мережі виникає збій або несправність, мережевий адміністратор повинен бути проінформований. Мережа повинна бути захищена, попереджаючи потенційні проблеми, перш ніж вони стануть основною проблемою. Методи, такі як SMS, E-mail та Pager, можуть бути використані для попередження адміністратора мережі щодо несправності в мережі.

Термін "моніторинг мережі" використовується для опису системи, яка допомагає постійно стежити за мережевою топологією, і виявляє будь-які перешкоди, сповільнення роботи системи або компонентів і негайно повідомляє менеджера мережі через електронну пошту, SMS або будь-які інші сигнали у випадку будь-яких проблем. Моніторинг мережі вважається непридатним, якщо не відстежуються потрібні речі. Звичайні області, що розглядаються, включають використання пропускної здатності, продуктивність сервера та продуктивність додатків. Серверний моніторинг є важливою частиною будь-якої архітектури моніторингу ЦОД, але занадто часто він стає важливим процесом успішної розробки цілісної платформи моніторингу. Моніторинг сервера - це моніторинг операційної системи та

пов'язаних із ним апаратних показників для серверів, які запускають програму. Це такий погляд на світ з точки зору сервера, але ніколи не з внутрішніх процесів. Основні показники моніторингу сервера включають час системи процесора, час очікування процесора, використовувана пам'ять, вільна пам'ять, довжина черги на диску, використання диску, швидкість передачі адаптера та ін. Контроль сервера використовується кожною IT-організацією у певній формі. Усі інструменти моніторингу запускаються за протоколом SNMP. Ринок з відкритим вихідним кодом включає в себе безліч варіантів, таких як Nagios, Cacti, Zenoss, Zabbix, Open NMS тощо. Основна потреба моніторингу залежить від типу бізнесу, що ведеться організацією. Там завжди була конкуренція між відкритим вихідним кодом та комерційними рішеннями, але багато компаній прагнуть придбати проекти з відкритим кодом, впроваджуючи різні варіанти проектів для комерційного та відкритого ринку. Розгортання різних параметрів, звітність, повідомлення; тригери, сповіщення, використання ресурсів тощо [16].

Nagios є найпопулярнішою системою моніторингу і складається з майже всіх дистрибутивів linux. Існують інші плагіни, додаткові скрипти, які можна налаштувати та використовувати разом з інструментом. Nagios - це програма легкої ваги та ідеальний інструмент моніторингу, який може допомогти контролювати всі активні протоколи та мережні пристрої, підключені до топології мережі. Він також здатний надавати в режимі реального часу комплексні графіки та аналіз тенденцій.

Програма «Cacti» є інструментом моніторингу продуктивності на базі стека LAMP (Linux / Apache / MySQL / PHP) і має RRD (Round Robin Database). Процеси, що проводяться в Cacti, включають збирання, управління та відображення графіків зібраних даних. Деякі дистрибутиви (наприклад, Fedora) також постачають версію у своїх сховищах. Cacti використовує технологію бази даних Round Robin (RRD) та бази даних MySQL для зберігання зібраної інформації. MySQL та PHP використовуються для надання графічного веб-інтерфейсу до баз даних RRD.

Програма Zenoss був розроблений Біллом, Еріком Далем та Марком Хінкле. Програма контролює всі пристрої, сервери, мережу та додатки всередині ЦОД. Основна база даних та події зберігаються в базі даних MySQL. Програма поставляється з інтегрованим пакетом, який містить всі комбіновані модулі.

Zabbix був розроблений Олексієм Владисьєвим і був випущений вперше в 2001 році. Поточна стабільна версія Zabbix - 1.8.3. Він може відстежувати основні служби SMTP, HTTP, ICMP без встановлення агентів. Zabbix має три основні модулі для його функціонування:

1. Демони;
2. Агенти;
3. Веб-інтерфейс.

3.4.2 Огляд програми Nagios

Однією з потужних систем моніторингу є Nagios. Nagios - це безкоштовний веб-монітор мережі з відкритим кодом, розроблений Ethan Galstad. Nagios призначений для роботи на Linux, але також може використовуватися в варіантах UNIX. Nagios відслідковує стан хост-систем та мережевих служб і повідомляє користувача про проблеми. Подібно до багатьох утиліт із відкритим кодом, установка вимагає певного ступеню досвіду системного адміністратора.

Nagios є основним інструментом, що використовується для діагностики, запобігання та вирішення мережевих проблем. Зростання високої пропускної спроможності та надзвичайно важливої міграції за допомогою локальної мережі (LAN) у широкосмуговій мережі (WAN) вимагає більш ефективних інструментів моніторингу. Без належних інструментів, які дозволяють аналізувати та відображати мережевий трафік та будь-яку пов'язану з ними проблему, мережевий адміністратор обмежується методом спроб і помилок, що триває багато часу, щоб спробувати визначити проблему. З широким спектром

функцій, включаючи ряд веб-інтерфейсів, Nagios - дуже корисний інструмент моніторингу, а так як велика кількість плагінів доступна в бібліотеці веб-монітору, то вона може бути налаштована відповідно до вимог. Необхідно зазначити, що Nagios здійснює моніторинг таких сервісів, як SMTP, POP3, HTTP, PING та такі ресурси, як використання диска та пам'яті, файли журналів, завантаження процесорів, що інтегрується з сенсором IT Temperature Monitor, що дозволяє контролювати і прогнозувати температуру серверної кімнати та пристрою за певними параметрами. Nagios дозволяє прогнозувати та моніторити, виникнення мережевого збою, недоступність хосту, і надає службові сповіщення. Nagios надає користувачам гнучкість у розробці власних чеків хоста та служби [15].

Основні можливості системи моніторингу:

- Моніторинг мережевих служб (SMTP, POP3, HTTP, NNTP, ICMP, SNMP);
- Моніторинг стану хостів (завантаження процесора, використання диска, системні логи);
- Підтримка віддаленого моніторингу через шифровані тунелі SSH або SSL;
- Проста архітектура модулів розширень (плагінів) дозволяє, використовуючи будь-яку мову програмування за вибором (Shell, C ++, Perl, Python, PHP, C # та інші), легко розробляти свої власні способи перевірки служб;
- Паралельна перевірка служб;
- Можливість визначати ієрархії хостів мережі за допомогою «батьківських» хостів, дозволяє виявляти і розрізняти хости, які вийшли з ладу, і ті, які недоступні;
- Відправлення сповіщень у разі виникнення проблем зі службою або хостом (за допомогою пошти, пейджера, смс, або будь-яким іншим способом, визначеним користувачем через модуль системи);

- Можливість визначати обробники подій, що відбулися зі службами або хостами для проактивного вирішення проблем;
- Автоматична ротація лог-файлів;
- Можливість організації спільної роботи декількох систем моніторингу з метою підвищення надійності і створення розподіленої системи моніторингу;
- Включає в себе утиліту nagiostats, яка виводить загальне зведення по всім хостам, за якими ведеться моніторинг.

Nagios - це мережевий інструмент реального часу, що використовується для аналізу, інтерпретації та відображення мережевого трафіку. Робоча станція та клієнт можуть відслідковувати певний потік трафіку в мережі, не порушуючи роботу мережі одночасно. Програма також надає інструменти для технічного контролю та ефективності роботи системи. Nagios демонструє використання пропускної здатності мережі, а також повідомляє адміністратора мережі по відповідно налаштованому ресурсу, якщо в мережі виникають певні проблеми з доступом або пропускна здатність потрапляє на певний поріг. Інтегрований MRTG також дає змогу адміністратору мережі переглядати завантаженість пропускної здатності під час пікових годин. Аналіз мережі в режимі реального часу допомагає швидко виявляти мережеві помилки та швидкодію, запобігаючи падінню мережі.

3.4.3 Основні переваги та недоліки системи моніторингу Nagios

Основним завданням Nagios є контроль стану мережевих пристроїв і їх служб, також повідомляти системних адміністраторів, коли було виявлені проблеми в мережі. Ядром Nagios є демон планувальника, який регулярно перевіряє зазначену мережу пристроїв та послуги, що вони надають. Коли виникають проблеми Nagios попереджає мережевих адміністраторів через канали повідомлень, таких як служба електронної пошти і миттєвих повідомлень. В свою чергу, мережевий адміністратор може відкрити веб-

інтерфейс для перегляду статусу інформації, журналів подій і звітів з будь-якого місця через доступ до інтернет мережі.

Система повідомлень може відправляти інформацію про будь-які відхилення в роботі контрольованих нею систем на адресу: IT-персоналу, бізнес підрозділів, а так же кінцевих користувачів по електронній пошті або використовуючи текстові повідомлення SMS, при цьому надаючи детальну інформацію про кожну подію, що трапилась. Для оперативного доступу до системи передбачена підтримка мобільних технологій: nagios xi android, nagios xi iOS.

Також слід зазначити, що Nagios має багатокористувацький доступ в веб-інтерфейс, надає всім зацікавленим особам, можливість отримувати інформацію про поточний стан всієї IT-інфраструктури підприємства. Призначений для користувача рівень доступу дозволяє бачити тільки дозволені до показу компоненти IT-інфраструктури. Одне з ключових переваг системи - можливість створення різних рівнів доступу до інформації. Це помітно спрощує управління акаунтами користувачів, а також адміністрування.

Веб-монітор Naios має потужний графічний інтерфейс забезпечує налаштування шаблонів, дизайну і переваг для кожного користувача, що так само створює додаткову гнучкість для членів команди користувачів системи.

Хоча гнучкість - це особливість, яка відрізняє Nagios від інших інструментів моніторингу, але все ж слід зазначити, що у Nagios все ж є певні слабкі місця. Наприклад, конфігурація системи заснована на складних текстових файлах. Інтерфейс самої системи не є інтерактивним, і можна сказати застарілим. Більш того, у Nagios немає інтегрованої бази даних минулих записів про продуктивність[17].

Плагін Nagios - автономний виконуваний файл, певний набір аргументів для виконання деяких дій і моніторингу. Існує два типи модулів, тобто контрольний плагін і плагін повідомлень. Nagios використовує результати перевірки плагінів для визначення поточного стану хостів і їх служб, в той час як модуль повідомлень використовується для відправки попереджень, при

зміні статусу хоста. На додаток до регулярних мережевих служби, такі як HTTP, FTP, SMTP, Nagios також можуть контролювати локальні ресурси, такі як завантаження і пам'ять ЦП використані через NRPE (Nagios Remote Plug-in Executor) розширення. Однією з найбільш гнучких особливостей Nagios є те, що вона дозволяє користувачам розробляти власні призначені плагіни.

Nagios надає API під назвою Nagios Event Broker (NEB), який дозволяє розробникам використати додатковий робочий потік до деяких типів подій Nagios. Наприклад, можна було б розробити модуль, в якому зберігаються результати перевірки, коли плагіни завершують виконання. Ці модулі підключаються до основного процесу, коли Nagios запускається так, що кожного разу, коли відбувається цільова подія, функція зворотного виклику в модулі буде викликатися. Таким чином, за допомогою модулів можна отримати всю необхідну інформацію в рамках основного процесу, такого як статус Nagios і перевірити результати. Але треба мати на увазі, що процес в модулі NEB може блокувати ядро Nagios, що може уповільнювати роботу всієї системи.

Nagios вимагає текстових файлів конфігурації, а створення таких файлів - непросте завдання. Користувачі повинні мати добре розуміння складної структури і запам'ятати всі параметри файлів Nagios для редагування з використанням звичайного текстового редактора, що є особливо важким і схильним до помилок при роботі з великою корпоративною мережею. Інструменти налаштування з відкритим вихідним кодом від спільноти Nagios може значно спростити цей процес. Прикладами цих інструментів є Lilac and Fruity, які мають PHP-інтерфейси для створення простих Nagios конфігурації[18]. Для більш складних конфігурацій NagiosQL і NConf пропонують такі функції корпоративного класу, як сервіс шаблонів, допомагаючи конфігурувати велика мережеві топології.

Сам же веб-інтерфейс Nagios був розроблений старомодним CGI з використанням мови програмування C. Додавання нових функції та редагування їх є вкрай незручними для розробників, тому що необхідна

компіляція. Крім того, досить складно інтегрувати з сучасними технологіями, такими як CSS, AJAX, JQuery і Flash. На щастя, модульна архітектура Nagios дозволяє замінювати деталі системи з їх, призначеними для користувача модулями.

3.4.4 Архітектура Nagios

Щоб запустити Nagios, нам потрібна машина з ОС Linux (або будь-який тип Unix) та компілятор мови C. CGI (Common Gateway Interface) необхідний у разі віддаленого моніторингу, що має дві передумови: веб-сервер (переважно Apache) та бібліотека для графічного дизайну динамічно створюваних зображень. Було впроваджено чотири типи файлів конфігурації, як на рисунку 3.4:

- Основний файл конфігурації, включаючи всі директиви, необхідні для демона Daemon;
- Файл ресурсів зберігає певні макроси користувача. Мета полягає в тому, щоб зберігати "чуттєві" конфігурації, такі як паролі, але не доступні для CGI;
- Визначення об'єкта. Файл містить описи для хостів, груп вузлів, контактів і т. д. Всі об’єкти, що потребують моніторингу, визначені тут. Один або декілька файлів використовуються для визначення цілей, описуючи ключові слова (директиви) "файл cfg" та / або "cfg_dir" в основній конфігурації;
- Конфігураційний файл CGI містить декілька директив, що визначають операційну систему CGI.

Nagios видає періодичні запити, запрограмовані плагінами. Значення, що повертаються можуть бути 0 для OK, 1 - для WARNING та 2 для CRITICAL.

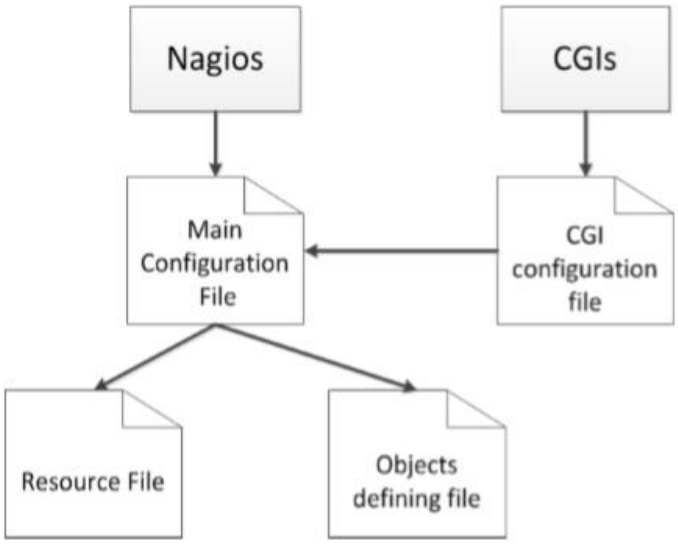

Рисунок 3.4 Конфігураційні файли та їх взаємодія

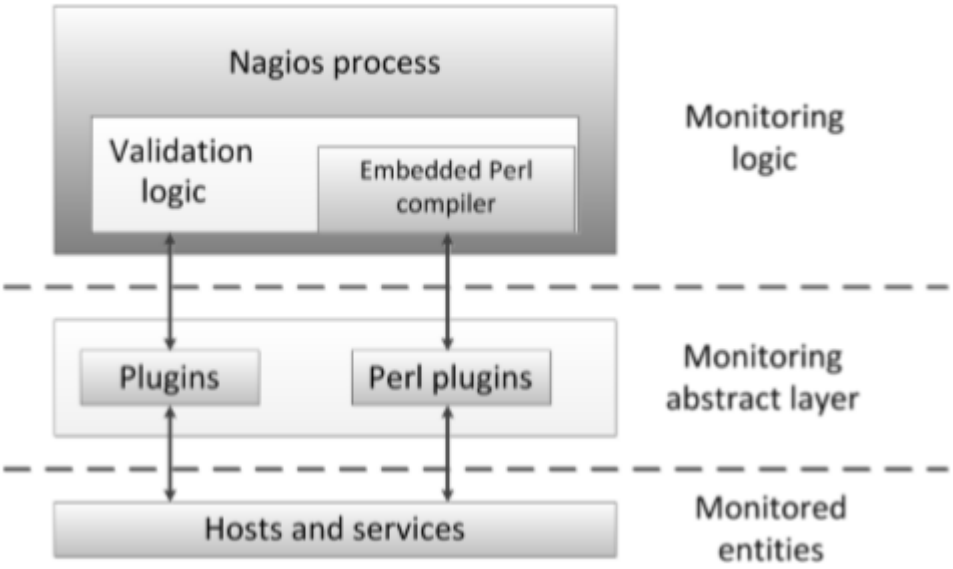

Рисунок 3.5 Логіка моніторингу

Сервер моніторингу потребує різних плагінів для контакту з віддаленими агентами залежно від операційної системи: check_nt та NSClient ++ для Windows (як на рисунку 3.6), а також check_nrpe та NRPE (Nagios Remote Plugin Executor) для Linux (як на рисунку 3.7).

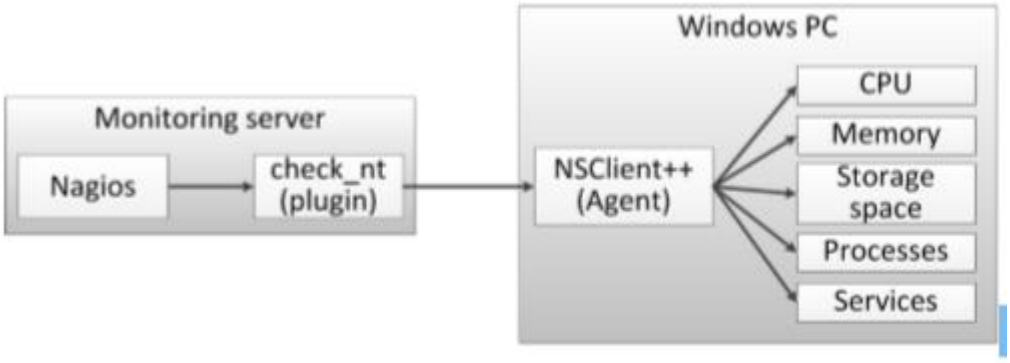

Рисунок 3.6 Моніторинг хоста запуску Windows

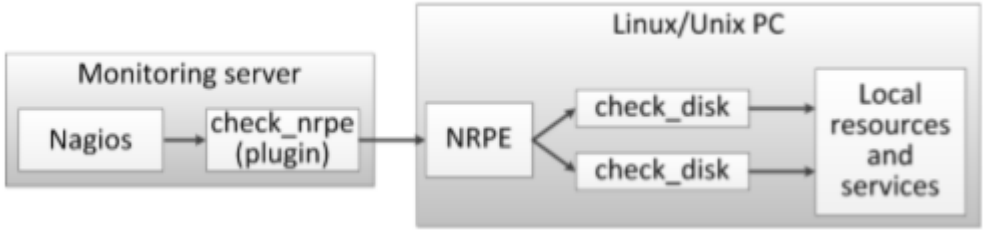

Рисунок 3.7 Моніторинг хоста під керуванням Linux / Unix

Windows-based NSClient ++ [19] - це простий, але потужний демон, який спочатку був створений для Nagios, прослуховуючи TCP-порт 12489. Однак він може бути налаштований для використання іншим інструментом моніторингу. Організований як служба, він зберігає плагіни у внутрішній стек, щоб надсилати запити або запити до інших плагінів. Цей інструмент моніторингу можна розширити, написавши новий плагін, запустивши зовнішній сценарій. NSClient ++ доступний для Windows NT4 / 2000 / XP / 2003 / Vista / 2008/7. Для останніх двох версій агент повинен запускати адміністратор користувача. З точки зору безпеки, віддалений моніторинг підтримується через SSH або SSL зашифровані тунелі.

Плагін check_nrpe на стороні сервера рекомендується для машин Linux / UNIX, і для цього потрібен NRPE. Однак цей плагін може працювати також з NSClient ++ (порт TCP 5666).

Порівнюючи NSClient ++ з NRPE, перший має багато готових до використання перевірок, які не вимагають від адміністратора запису інших

сценаріїв. З іншого боку, встановлення чистого NRPE вимагає лише зовнішніх сценаріїв.

3.5 Висновки до розділу 4

У даному розділі було:

1. Вибрано та описано основний елемент – Raspberry Pi, що використовується про створенні макета.
2. Вибрано та описано систему моніторингу Nagios, що використовувались при створенні макета.

Raspberry Pi - це мініатюрна, і зручна платформа швидкої розробки електронних пристроїв для новачків і професіоналів, розміром з кредитну карту, ультра дешевий комп'ютер, створений Девідом Брабеном.

Виділено наступні основні перевагі одноплатних комп’ютерів:

- Висока продуктивність.
- Малі габарити.
- Низька собівартість.
- Простота налаштування.
- Можливість використання великого числа додаткових модулів.

Виділено основні можливості, недоліки та переваги системи моніторингу Nagios:

- Моніторинг мережевих служб (SMTP, POP3, HTTP, NNTP, ICMP, SNMP);
- Моніторинг стану хостів (завантаження процесора, використання диска, системні логи);
- Підтримка віддаленого моніторингу через шифровані тунелі SSH або SSL;
- Проста архітектура модулів розширень (плагінів) дозволяє, використовуючи будь-яку мову програмування за вибором (Shell, C ++, Perl,

Python, PHP, C # та інші), легко розробляти свої власні способи перевірки служб;

- Паралельна перевірка служб;
- Можливість визначати ієрархії хостів мережі за допомогою «батьківських» хостів, дозволяє виявляти і розрізняти хости, які вийшли з ладу, і ті, які недоступні;
- Відправлення сповіщень у разі виникнення проблем зі службою або хостом (за допомогою пошти, пейджера, смс, або будь-яким іншим способом, визначеним користувачем через модуль системи);
- Можливість визначати обробники подій, що відбулися зі службами або хостами для проактивного вирішення проблем;
- Автоматична ротація лог-файлів;
- Можливість організації спільної роботи декількох систем моніторингу з метою підвищення надійності і створення розподіленої системи моніторингу.

РОЗДІЛ 4. СТВОРЕННЯ МАКЕТА РЕЛІЗАЦІЇ СИСТЕМИ МОНІТОРИНГУ ДЛЯ ЦЕНТРІВ ОБРОБКИ ДАНИХ

4.1 Необхідні елементи для створення макетів

Для конструювання макету необхідно пройти ряд етапів пов’язаних з безпосереднім конструюванням макету та зі створенням відповідних програмних модулів.

Для встановлення системи моніторингу на одноплатний комп’ютер будуть використанні наступні елементи:

- Центральний вузол – Raspberry Pi 3 Model B +;
- ОС Raspbian;
- Система моніторингу – програма Nagios;
- Графічна бібліотека GD-Utils;
- Web-сервер Apache;

Для конструювання макету необхідно:

- Налаштування та встановлення програмного забезпечення Nagios;
- Встановлення ОС Raspbian;
- Встановлення GD-Utils;
- Конфігурація сервера Apache;
- Підключити центральний вузол до мережі та перевірити його доступність та доступність системи моніторингу.

Для встановлення веб-монітору Nagios на сервер необхідні наступні елементи:

- Центральний вузол - HP PROLIANT DL120 G5;
- ОС Ubuntu;
- Система моніторингу – програма Nagios;
- Web-сервер Apache;
- Підключити центральний вузол до мережі та перевірити його доступність та доступність системи моніторингу.

Для конструювання макету необхідно:

- Налаштування та встановлення програмного забезпечення Nagios;
- Встановлення ОС Ubuntu;
- Конфігурація сервера Apache;
- Підключити центральний вузол до мережі та перевірити його доступність та доступність системи моніторингу.

4.2. Конструювання макету з центральним вузлом - Raspberry Pi 3 Model B+

4.2.1 Огляд Raspberry Pi 3 Model B+

Комп'ютер Raspberry Pi 3 Model B+ розміром з банківську карту має на платі звичні ПК складові: процесор, оперативну пам'ять, роз'єм HDMI, композитний вихід, USB, Ethernet, Wi-Fi і Bluetooth.

Головна перевага Raspberry Pi - 40 контактів введення / виведення загального призначення (GPIO). До них ми зможемо підключати периферію для взаємодії із зовнішнім світом: виконавчі пристрої, будь-які сенсори і все, що працює від електрики.

Штатною операційною системою для Raspberry Pi є Linux. Вона встановлюється на microSD карту, а та - в спеціальний слот на платі.

Raspberry Pi 3 Model B + має 64-х бітовий чотирьохядерний процесор ARM Cortex-A53 розігнаний з 1,2 ГГц до 1,4 ГГц. На платі модернізовані бездротові інтерфейси Wi-Fi 802.11n і Bluetooth 4.2 / LE. Крім того, процесор має архітектуру ARMv53, а значить ми зможете використовувати різні операційні системи: Debian Wheezy, Ubuntu Mate, Fedora Remix і навіть MS Windows 10 IoT.

Для підключення монітора або телевізора використовується композитний відеовихід або роз'єм HDMI. Дозвіл варіюється від 640 × 350 (EGA) до 1920 × 1200 (WUXGA) для HDMI. Композитний вихід працює в форматах PAL і NTSC. Колонки або навушники підключаються через

стандартне гніздо 3,5 мм. Також звук може передаватися по HDMI. Raspberry Pi 3 Model B + надає 4 USB-портів, об'єднаних внутрішнім хабом. До них, крім іншого, можна підключити клавіатуру і мишу.

Для економії ресурсів центрального процесора, Raspberry Pi пропонує підключення штатних модулів через 15-пінові слоти:

- CSI-2 - для підключення камери по інтерфейсу MIPI;
- DSI - для підключення штатного дисплея.

В якості низькорівневих інтерфейсів доступні:

- 40 портів введення-виведення загального призначення;
- UART ;
- I²C / TWI;
- SPI з селектором між двома пристроями;
- Піни живлення: 3,3 В, 5 В і земля.

Для комунікації на Raspberry Pi 3 Model B доступні інтерфейси Ethernet на 10/100/1000 Мбіт з виходом на стандартне гніздо 8P8C (RJ45), Wi-Fi 802.11n і Bluetooth 4.2.

Живлення Raspberry Pi 3 здійснюється від 5-вольтового адаптера через роз'єм micro-USB або піни живлення.

Апаратний вимикач живлення на платі відсутній. Для включення комп'ютера досить підключити кабель живлення. Для виключення використовуються штатні функції операційної системи.

Замість традиційного для звичайних комп'ютерів жорсткого диска, Raspberry Pi використовує microSD флеш-карту. Вона повинна бути попередньо підготовлена - на неї слід встановити операційну систему. Маючи кілька флеш-карт, ми можемо по черзі використовувати їх, отримавши кілька ізольованих образів комп'ютерів.

На Raspberry Pi 3 Model B + поліпшили управління температурою SoC, цьому також сприяє металева кришка. Нижче 70 ° C використовуються поліпшення для збільшення частоти ядра до 1.4 ГГц. При температурі вище

70 ° С частота падає до 1.2 ГГц, а також зменшується і напруга ядра, тим самим збільшується час до досягнення критичної температури в 80 ° С[13].

Таблиця 4.1 Технічні характеристики Raspberry Pi 3 Model B+

Система на кристалі (SoC)	Broadcom BCM2837B0 (CPU + GPU + RAM)
процесор	64-бітний чотирьохядерний ARMv8 Cortex-A53 процесор з тактовою частотою 1.4 ГГц; 16 КБ cache L1 і 512 КБ cache L2
Графічний процесор	Двоядерний процесор (GPU) VideoCore IV (3D GPU @ 300 МГц, відео GPU @ 400 МГц) підтримує стандарти OpenGL ES 2.0, OpenVG, MPEG-2, VC-1 і здатний кодувати, декодувати і виводити Full HD-відео (1080p, 30 FPS, H.264 High-Profil)
ОЗП	1 ГБ SDRAM LPDDR2
Сховище	слот для карти пам'яті MicroSD
Цільова ціна	$ 35
Etherne	10/100/1000 Мбіт Gigabit Ethernet (через USB 2.0) (контролер LAN7515 - USB 2.0 Hub і Ethernet)
Wi-Fi / Bluetooth	2.4 ГГц і 5 ГГц IEEE 802.11.b / g / n / ac WI-FI і Bluetooth 4.2 Low Energy (BLE), що забезпечуються мікросхемою Cypress CYW43455
Відео вхід	1 x CSI-2 для підключення камери по інтерфейсу MIPI

Продовження Таблиці 4.1 Технічні характеристики Raspberry Pi 3 Model B+

Відео вихід	1 x DSI (Display Serial Interface) для підключення штатного дисплея; 1 x композитний відеовихід (CVBS відео, PAL і NTSC) 3.5 мм роз'єм
Аудіо вхід	Ні, але можна додати USB-мікрофон або звукову карту
Аудіо вихід	гніздо 3.5 мм, HDMI
USB-порти	4 порти USB 2.0 через USB hub в Microchip LAN7515
Периферія	40 портів введення-виведення загального призначення (GPIO), UART (Serial), I²C / TWI, SPI з селектором між двома пристроями
Живлення	Живлення 5 В, 2.5 А через порт micro-USB або GPIO; Power over Ethernet (PoE) через окремий PoE HAT
Розміри	85.6 мм x 56.5 мм x 17 мм
ОС	Ubuntu, Debian, Fedora, Arch Linux, Gentoo, RISC OS, Android, Firefox OS, NetBSD, FreeBSD, Slackware, Tiny Core Linux, Windows 10 IOT

4.2.2 Встановлення графічної бібліотеки GD

GD – відкрита бібліотека з вихідним кодом для динамічного створення зображень програмістами. GD створює зображення форматів PNG, JPEG, GIF та WBMP. GD дозволяє створювати зображення із ліній, дуг, тексту і інших

зображень, а також використовувати різні кольори. Дану бібліотеку зазвичай використовують для створення діаграм, графіків, ескізів та ін.

Для нормального функціонування системи моніторингу – Nagios дана бібліотека є необхідністю так як сама система моніторингу побудована га графіках та діаграмах. Так як бібліотека є відкритою то для нашого макета можна просто встановити образ GD в домашню директорію центрального вузла де і відбувається встановлення самої системи моніторингу.

Лістінг 4.1 Встановлення GD-Utils

root@raspberrypi:/tmp# wget
http://www.boutell.com/gd/http/gd-2.0.33.tar.gz

root@raspberrypi:/tmp# tar –zxvf gd-2.0.33.tar.gz

root@raspberrypi:/tmp/gd-2.0.33# make && make install

4.2.3 Встановлення web-серверу Apache

Apache - це повнофункціональний, розширюваний веб-сервер, що повністю підтримує протокол HTTP/1.1 і поширюється з відкритим вихідним кодом. Web-сервер Apache є самостійним, некомерційним, вільно розповсюджуваним продуктом. Продукт підтримує безліч можливостей, багато з яких реалізовані як скомпільовані модулі, які розширюють основні функціональні можливості. Вони різняться від серверної підтримки мов програмування до схем аутентифікації. Існують інтерфейси для підтримки мов програмування Perl, Python, Tcl і PHP. Сервер може працювати практично на всіх поширених платформах. Існують готові виконувані файли сервера для Windows NT, Windows 9x, OS / 2, Netware 5.x і декількох UNIX-систем. При цьому він дуже простий в установці і конфігурації.

Найпростіша функція, яку може виконувати Apache - стояти на сервері і обслуговувати звичайний HTML-сайт. При отриманні запиту на певну сторінку сервер відправляє в її відповідь браузеру.

За допомогою сервера Apache можна виробляти просту аутентіфікацію. Функція, яка закладена в протоколі HTTP / 1.1 - аутентифікація користувачів. За допомогою штатних засобів сервера Apache можна розмежувати доступ до певних сторінок сайту для різних користувачів. Це потрібно, наприклад, для того щоб зробити адміністраторський інтерфейс до сайту. Користувачі можуть бути розбиті на групи, і для кожної з них можна призначити свої права доступу.

Популярні методи стискування на Apache включають зовнішній модуль mod_gzip, створений для зменшення розміру веб-сторінок, переданих по HTTP.

Функції віртуального хостингу дозволяють одній інсталяції Apache обслуговувати різні веб-сайти.

Лістинг 4.2 Встановлення серверу Apache

root@raspberrypi:/tmp/nagios# make all

root@raspberrypi:/tmp/nagios# make install-webconf

root@raspberrypi:/tmp/nagios#
/etc/init.d/apache2reload

4.2.4 Встановлення Nagios на центральний вузол макета

Nagios - це безкоштовний веб-монітор мережі з відкритим кодом, розроблений Ethan Galstad. Nagios призначений для роботи на Linux, але також може використовуватися в варіантах UNIX. Nagios відслідковує стан хост-систем та мережевих служб і повідомляє користувача про проблеми. Подібно

до багатьох утиліт із відкритим кодом, установка вимагає певного ступеню досвіду системного адміністратора.

Першим кроком для виконання цього пункту э встановлення операційної системи Raspbian на одноплатний комп`ютер Raspberry Pi, який виступає центральним вузлом нашого макету. Raspbian має завчасно скомпільований пакет Nagios. Наступними кроками є встановлення необхідних пакетів перед компіляцією Nagios та створення груп користувачів та користувачів Nagios.

Лістинг 4.3 Загальний вигляд команд початкових кроків для встановлення Nagios на Raspberry Pi

```
root@raspberrypi:/home/pi# sudo apt-get update
root@raspberrypi:/home/pi# sudo apt-get install php5 apache2
libgd2-xpm libgd2-xpm-dev libgd2-dev libpng12-dev libjpeg62-dev
libgd-tools libpng12-dev libgd2-xpm libgd2-xpm-dev libssl-dev
gnutls-bin iputils

root@raspberrypi:/home/pi# groupadd www-data
root@raspberrypi:/home/pi# groupadd nagios
root@raspberrypi:/home/pi# adduser nagios
root@raspberrypi:/home/pi# usermod -G nagios nagios
root@raspberrypi:/home/pi# usermod -G www-data,nagios www-data
root@raspberrypi:/tmp# wget http://prdownloads.sourceforge.net
/sourceforge/nagios/nagios-3.4.1.tar.gz

root@raspberrypi:/tmp# tar xzf nagios-3.4.1.tar.gz
root@raspberrypi:/tmp/nagios# ./configure –prefix=/usr/local
/nagios –with-cgiurl=/nagios/cgi-bin –with-htmurl=/nagios/
–with-nagios-user=nagios –with-nagios-group=nagios
–with-command-group=nagios
```

root@raspberrypi:/tmp/nagios# make install
root@raspberrypi:/tmp# wget http://prdownloads.sourceforge.net
/sourceforge/nagiosplug/nagios-plugins-1.4.15.tar.gz

root@raspberrypi:/tmp# tar xzf nagios-plugins-1.4.15.tar.gz
root@raspberrypi:/tmp/nagios-plugins-1.4.15# ./configure
root@raspberrypi:/tmp/nagios-plugins-1.4.15# make && make

4.2.5 Підключення центрального вузла та перевірка доступності вузлів мережі

Для підключення центрального вузла до мережі нема необхідності використання додаткових модулів оскільки інтерфейс Ethernet уже вмонтований на плату.

Усі вузли (якщо такі наявні) макету знаходяться в одній підмережі. Найпростішим способом перевірки доступності вузлів є використання команди ping.

Далі запускаємо програму Nagios та перевіряємо її повноцінну роботу.

Лістинг 4.4 Запуск Nagios з центрального вузла
root@raspberrypi:/tmp# service nagios start

4.3 Конструювання макету з центральним вузлом - сервером HP Proliant DL120 G5

4.3.1 Загальні технічні характеристики серверу - HP Proliant DL120 G5

Розглянемо основні технічні характеристики серверу[20] в Таблиці 4.2.

Таблиця 4.2 Технічні характеристики серверу HP Proliant DL120 G5

Процесор	Двоядерний процесор Intel® Xeon® E3110
Шина FSB процесора	Шина FSB 1333/1066/800 МГц
Стандартне ОЗП	1 Гб або 2 Гб
Тип пам'яті	Небуферизована пам'ять PC2-6400 (800 МГц) ECC DDR2 SDRAM з підтримкою чергування адрес (якщо модулі DIMM розміщуються парами)
Максимальна пам'ять	8 Гб
Слоти для пам'яті	4 слотів DIMM
функції живлення	Блок живлення з автоматичним визначенням, 350 Вт, PFC, відповідність CE Марк
Зовнішні порти введення-виведення	Послідовний - 1; USB 2.0 - 5 (2 спереду, 1 внутрішній, 2 ззаду); графічний - 1 (ззаду); Клавіатура - 1; Миша - 1; Управління - 1 для додаткового LO100c; мережевий RJ-45 - 1
Мережевий інтерфейс	Вбудований NC105i гігабітний серверний адаптер
Сумісні операційні системи	Windows® Server 2003 (web, standard і enterprise edition standard і enterprise editions); Microsoft® Windows® 2008; Red Hat Enterprise Linux; SUSE Linux Enterprise Server

Продовження Таблиці 4.2 Технічні характеристики серверу HP Proliant DL120 G5

Функції управління	ASR (Automatic Server Recovery); Вбудований журнал управління; Монітор контролю параметрів накопичувача (з контролерами Smart Array); Функція динамічного відновлення секторів (з контролерами Smart Array); Профілактична гарантія на процесори, пам'ять і жорсткі диски SAS; Послідовна консоль BIOS; Передня і задня кнопки / індикатори Unit ID (UID)
Управління безпекою	Пароль увімкнення; Пароль клавіатури; контроль порту USB; Знімний комплект DVD-ROM Drive Assembly (опція); порт мережевого контролера LO100c (додатково); пароль адміністратора
Вага без упаковки	14,00 кг

4.3.2 Встановлення системи моніторингу Nagios на центральний вузол - HP PROLIANT DL120 G5

Перед початком встановлення системи моніторингу на сервері нам потрібно зайти на офіційний сайт Nagios - www.nagios.org, там ми бачимо список версій, та на необхідній натискаємо правою клавішею миші і копіюємо посилання необхідної нам версії як на рисунку нижче.

Nagios Core

Latest Version 4 Releases

Version	Date	Notes	Type	Link
4.4.1	2018-06-25	Latest stable release	Source code	nagios-4.4.1.tar.gz
4.4.0	2018-06-19	Previous stable release	Source code	nagios-4.4.0.tar.gz
4.3.4	2017-08-24	Previous stable release	Source code	nagios-4.3.4.tar.gz
4.2.4	2016-12-07	Previous stable release	Source code	nagios-4.2.4.tar.gz

Рисунок 4.1 Приклад доступних версій Nagios

Далі скачуємо файли на сервер за допомогою команди wget, наперед обравши зручну для себе папку для скачування, як зображено на рисунку 4.2.

```
root@server:~# cd /home/mariyka/
root@server:/home/mariyka# wget https://assets.nagios.com/downloads/nagioscore/releases/nagios-4.4.1.tar.gz
--2018-08-05 18:07:34--  https://assets.nagios.com/downloads/nagioscore/releases/nagios-4.4.1.tar.gz
Resolving assets.nagios.com (assets.nagios.com)... 2600:3c00::f03c:91ff:fedf:b821, 72.14.181.71
Connecting to assets.nagios.com (assets.nagios.com)|2600:3c00::f03c:91ff:fedf:b821|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 11296403 (11M) [application/x-gzip]
Saving to: 'nagios-4.4.1.tar.gz'

100%[=====================================================================>] 11,296,403  2.96MB/s   in 4.3s

2018-08-05 18:07:44 (2.52 MB/s) - 'nagios-4.4.1.tar.gz' saved [11296403/11296403]

root@server:/home/mariyka# wget https://nagios-plugins.org/download/nagios-plugins-2.2.1.tar.gz
--2018-08-05 18:08:16--  https://nagios-plugins.org/download/nagios-plugins-2.2.1.tar.gz
Resolving nagios-plugins.org (nagios-plugins.org)... 72.14.186.43
Connecting to nagios-plugins.org (nagios-plugins.org)|72.14.186.43|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2728818 (2.6M) [application/x-gzip]
Saving to: 'nagios-plugins-2.2.1.tar.gz'

100%[=====================================================================>] 2,728,818   1.47MB/s   in 1.8s

2018-08-05 18:08:18 (1.47 MB/s) - 'nagios-plugins-2.2.1.tar.gz' saved [2728818/2728818]
```

Рисунок 4.2 Встановлення файлу версії Nagios на сервер

Далі нам необхідно розпакувати скачаний файл Nagios і зайти в нього, після чого ми приступаємо до компіляції.

Лістинг 4.5 Розпакування файлу та його компіляція

root@server:/home/mariyka# tar xzf nagios-4.4.1.tar.gz

root@server:/home/mariyka# cd nagios-4.4.1/

root@server:/home/mariyka/nagios-4.4.1# ./configure –with-command-group=nagcmd

root@server:/home/mariyka/nagios-4.4.1# make all

Встановлення плагінів для системи моніторингу відбувається по такому ж принципу, його можна побачити на лістингу 4.6.

Лістинг 4.6 Встановлення плагінів Nagios

root@server:/home/mariyka/nagios-plugins-2.2.1#

root@server:/home/mariyka/nagios-plugins-2.2.1# ./configure --with-nagios-user=nagios –with-nagios-group=nagios

Далі ми додаємо роутери, ПК та маршрутизатори для моніторингу, які нам необхідні, як зображено на лістингу 4.7. Ми створимо три файли, routers.cfg, switches.cfg, і pcs.cfg, і створюємо записи для об’єднання в класи.

Лістинг 4.7 Встановлення ПК в моніторинг

```
define host {
   use             generic-host
   host_name  Duty2
   alias           PC
   address     172.20.10.154
}
```

Таким чином мною було створено для моніторингу 52 хостів та 82 сервісів, що зображено на рисунку 4.3-4.5.

Рисунок 4.3 Кількість хостів та сервісів, що стоять в моніторингу

Host Status Details For All Host Groups
Entries sorted by **state duration** (descending)

Limit Results: 100

Host	Status	Last Check	Duration	Status Information
localhost	UP	12-04-2018 20:48:39	58d 6h 37m 35s	PING OK - Packet loss = 0%, RTA = 0.02 ms
support-sw	UP	12-04-2018 20:44:45	18d 10h 53m 11s	PING OK - Packet loss = 0%, RTA = 3.48 ms
Strix	UP	12-04-2018 20:48:09	5d 10h 58m 6s	PING OK - Packet loss = 0%, RTA = 0.90 ms
Duty	UP	12-04-2018 20:46:31	1d 12h 59m 56s	PING OK - Packet loss = 0%, RTA = 0.81 ms
Duty2	UP	12-04-2018 20:46:47	0d 12h 47m 12s	PING OK - Packet loss = 0%, RTA = 0.83 ms
Duty3	UP	12-04-2018 20:48:28	0d 12h 46m 4s	PING OK - Packet loss = 0%, RTA = 27.02 ms
Fedya	UP	12-04-2018 20:48:18	0d 12h 9m 48s	PING OK - Packet loss = 0%, RTA = 0.25 ms
Duble1	UP	12-04-2018 20:48:00	0d 0h 49m 2s	PING OK - Packet loss = 0%, RTA = 0.18 ms
Duble2	UP	12-04-2018 20:48:19	0d 0h 48m 46s	PING OK - Packet loss = 0%, RTA = 0.17 ms
Duble3	UP	12-04-2018 20:48:21	0d 0h 45m 46s	PING OK - Packet loss = 0%, RTA = 0.17 ms
Duble5	UP	12-04-2018 20:48:18	0d 0h 39m 41s	PING OK - Packet loss = 0%, RTA = 0.23 ms
Duty4	DOWN	12-04-2018 20:45:08	0d 0h 38m 21s	CRITICAL - Host Unreachable (217.20.191.8)
Duble10	UP	12-04-2018 20:48:06	0d 0h 37m 54s	PING OK - Packet loss = 0%, RTA = 0.20 ms

Рисунок 4.4 Приклад хостів, що стоять в моніторингу

Service Status Details For All Hosts
Entries sorted by **state duration** (descending)

Limit Results: 100

Host	Service	Status	Last Check	Duration	Attempt	Status Information
localhost	Current Load	OK	12-04-2018 20:46:43	58d 6h 38m 12s	1/4	OK - load average: 0.00, 0.00, 0.00
	Current Users	OK	12-04-2018 20:49:17	58d 6h 37m 34s	1/4	USERS OK - 2 users currently logged in
	HTTP	OK	12-04-2018 20:46:27	58d 6h 36m 57s	1/4	HTTP OK: HTTP/1.1 200 OK - 11783 bytes in 0.000 second response time
	PING	OK	12-04-2018 20:49:41	58d 6h 36m 19s	1/4	PING OK - Packet loss = 0%, RTA = 0.02 ms
	Root Partition	OK	12-04-2018 20:48:20	58d 6h 35m 42s	1/4	DISK OK - free space: / 213223 MB (99.16% inode=99%):
	SSH	OK	12-04-2018 20:45:10	58d 6h 35m 4s	1/4	SSH OK - OpenSSH_6.6.1p1 Ubuntu-2ubuntu2.7 (protocol 2.0)
	Swap Usage	OK	12-04-2018 20:48:27	58d 6h 34m 27s	1/4	SWAP OK - 100% free (8188 MB out of 8188 MB)
	Total Processes	OK	12-04-2018 20:45:38	58d 6h 33m 49s	1/4	PROCS OK: 69 processes with STATE = RSZDT
Duty	Check_vlan2	OK	12-04-2018 20:48:59	1d 13h 1m 13s	1/4	PING OK - Packet loss = 0%, RTA = 0.19 ms
Duty2	Check_vlan2	OK	12-04-2018 20:46:46	0d 12h 48m 29s	1/4	PING OK - Packet loss = 0%, RTA = 0.18 ms
Duty3	Check_vlan2	OK	12-04-2018 20:49:19	0d 12h 47m 21s	1/4	PING OK - Packet loss = 0%, RTA = 0.17 ms
Duty	Check_dubl57	OK	12-04-2018 20:47:09	0d 0h 18m 3s	1/4	PING OK - Packet loss = 0%, RTA = 0.13 ms
	Check_dubl15	OK	12-04-2018 20:47:14	0d 0h 17m 58s	1/4	PING OK - Packet loss = 0%, RTA = 0.15 ms
	Check_dubl19	OK	12-04-2018 20:47:47	0d 0h 17m 25s	1/4	PING OK - Packet loss = 0%, RTA = 0.16 ms
	Check_dubl46	OK	12-04-2018 20:47:51	0d 0h 17m 21s	1/4	PING OK - Packet loss = 0%, RTA = 0.16 ms
	Check_dubl39	OK	12-04-2018 20:47:54	0d 0h 17m 18s	1/4	PING OK - Packet loss = 0%, RTA = 0.14 ms
	Check_dubl1	OK	12-04-2018 20:48:00	0d 0h 17m 12s	1/4	PING OK - Packet loss = 0%, RTA = 0.14 ms
	Check_dubl31	OK	12-04-2018 20:48:03	0d 0h 17m 9s	1/4	PING OK - Packet loss = 0%, RTA = 0.16 ms
	Check_dubl59	OK	12-04-2018 20:48:15	0d 0h 16m 57s	1/4	PING OK - Packet loss = 0%, RTA = 0.15 ms
	Check_vlandown	CRITICAL	12-04-2018 20:46:38	0d 0h 16m 45s	4/4	CRITICAL - Host Unreachable (172.16.0.155)
	Check_dubl48	OK	12-04-2018 20:48:37	0d 0h 16m 35s	1/4	PING OK - Packet loss = 0%, RTA = 0.15 ms
	Check_dubl5	OK	12-04-2018 20:49:09	0d 0h 16m 3s	1/4	PING OK - Packet loss = 0%, RTA = 0.15 ms
	Check_dubl40	OK	12-04-2018 20:49:13	0d 0h 15m 59s	1/4	PING OK - Packet loss = 0%, RTA = 0.28 ms
	Check_dubl22	OK	12-04-2018 20:49:14	0d 0h 15m 58s	1/4	PING OK - Packet loss = 0%, RTA = 0.11 ms
	Check_dubl13	OK	12-04-2018 20:49:17	0d 0h 15m 55s	1/4	PING OK - Packet loss = 0%, RTA = 0.15 ms

Рисунок 4.5 Приклад сервісів, що стоять в моніторингу

Після встановлення хостів та сервісів на моніторинг, що вказані на рисунку 4.4-4.5, за допомогою утиліти htop було знято показники завантаженості системи, що можна побачити на рисунку 4.6.

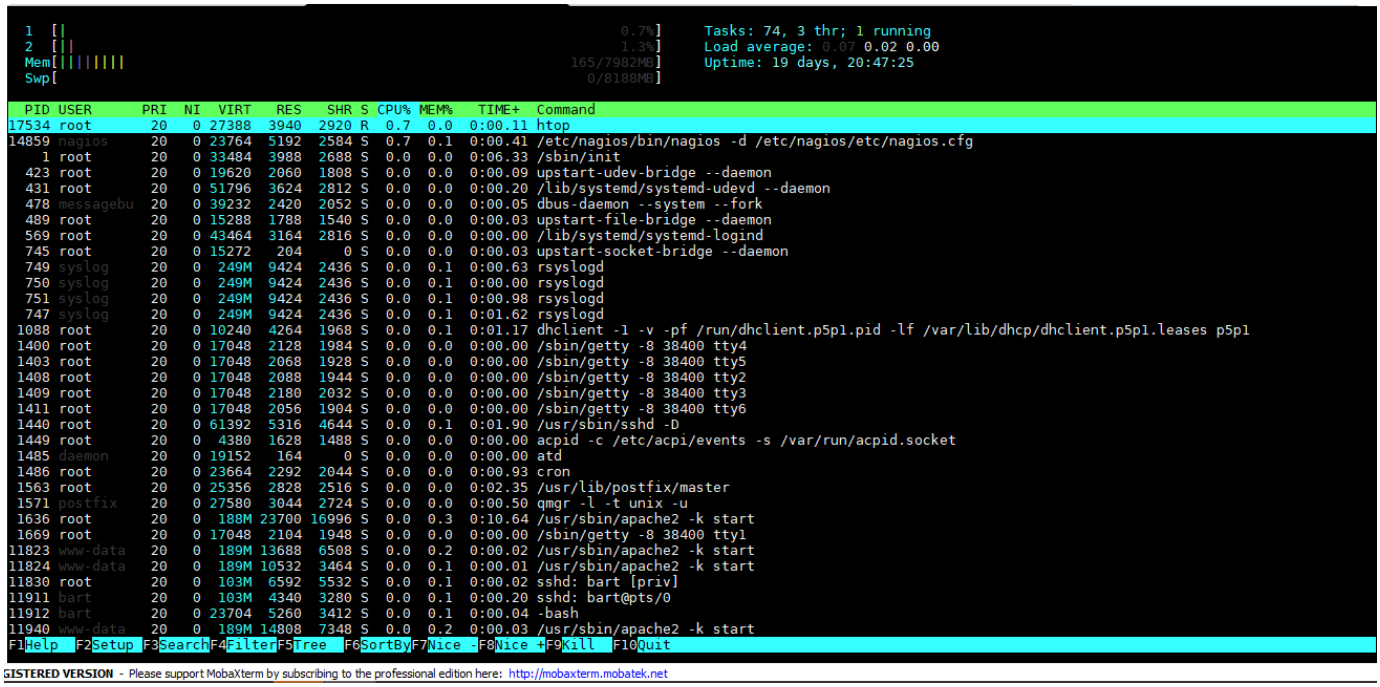

Рисунок 4.6 Виконання утиліти htop на сервері

Htop показує динамічний список системних процесів, список зазвичай вирівнюється по використанню ЦПУ. На відміну від top, htop показує всі процеси в системі. Також показує час безперервної роботи, використання процесорів і пам'яті. Htop часто застосовується в тих випадках, коли інформації дається утилітою top недостатньо, наприклад при пошуку витоків пам'яті в процесах. Htop написаний на мові C і використовує для відображення бібліотеку Ncurses.

Загалом показники завантаженості ЦП не перевищували 1.5%, середній показник – 0.7%

4.4 Система моніторингу Nagios, що реалізована на сервері в умовах проходження трафіку та процесів реального ЦОД

Для отримання реальних показників було проведено тестування в умовах реального Інтернет-провайдеру WNET та DOMONET (дочірній філіал

компанії WNET). Компанія WNET для моніторингу своєї мережі використовую систему моніторингу Nagios, що встановлений на сервері DELL PowerEdge 2950, що встановлений в їх ЦОД [21].

Таблиця 4.3 Технічні характеристики серверу DELL PowerEdge 2950

Виробник	DELL
Обсяг оперативної пам’яті	8 Гб
Максимальний обсяг оперативної пам’яті	32 Гб
Тип пам'яті оперативної пам’яті	DDR2
Частота шини	667 МГц
Кількість роз'ємів	8
Підтримка RAID	RAID 0/1
Тип приводу	DVD / CD-PB
Операційна система	Ubuntu 14.04.3
Потужність блоку живлення	2 x 750 Вт
Розміри (ШхВхГ)	744 x 444 x 864 мм
Вага	23 кг
Центральний процесор	2
Модель CPU	Intel Xeon E5450
Тактова частота CPU	3.0 Ггц
Обсяг жорсткого диску	120Гб
USB	6
RJ45 (LAN)	2
Monitor port (VGA)	є
PS / 2	є

Даний агрегат є 2U стійким сервером, а також є гнучкою основою для всієї інформаційної інфраструктури компанії. Передня панель сервера, на якому розташовані два порти USB 2.0, вихід VGA, LCD-панель, а також приводи DVD або CD. Внизу є роз'єми для жорстких дисків 3,5 і 2,5 дюйма.

Кнопка включення розташована тут же, на LCD-панелі. Всі найбільш часто використовувані кнопки та роз'єми знаходяться в абсолютному доступі, що гарантує легкість у використанні сервера.

На задній панелі також розташовано багато чого цікавого. Так тут знаходиться порт (RJ-45), що дозволяє підключати плату дистанційного доступу (DRAC5), ще два порта USB і VGA-вихід, COM-порт. Окрім цього є 2 мережевих інтерфейсів по 1 Гбіту і блоки живлення. 3 слота різьблення дозволяють встановити додаткові плати для розширення.

Що стосується процесора, то встановлені 2 процесори Intel Xeon 5450 з частотою 3 Ггц. В DELL PowerEdge 2950 можна встановити до 32 Гбайт пам'яті, розмістивши в восьми DIMM слотах плати пам'яті FBDIMM DDR2, частотою 533 Мгц або 667 Мгцц. Підсистема пам'яті сервера даної моделі є можливістю для розширення через різні модифікації. Також є можливість встановити RAID-контролер (PERC5 / I), якщо ви плануєте працювати з RAID-масивами.

Що стосується системи охолодження, то вона представлена шести вентиляторами, кожна з яких 60 мм в діаметрі. Два вентилятора встановлені безпосередньо в блоках живлення. Так само чотири кулери встановлені перед процесорними радіаторами, доступ до яких можна отримати, просто знімаючи пластикову кришку. Вентилятори представляють собою картриджі, кожен з яких можна легко оновити, завдяки функції гарячого замінника. Заміну картриджів можна зробити без перебою роботи серверу.

Живлення сервера забезпечує блок на 750 Вт з функцією «гаряча заміна». Хоча в базовій комплектації всього один блок живлення, можна додатково встановити ще один, що підвищить відмовостійкість всієї системи.

Сервер оснащений достатнім числом слотів, в які можна встановити різні плати розширення. Так ми можемо встановити 3 PCI-слота і 3 PCI-Express

(один x4 і два x8), або, як варіант, два PCI-X 64bit / 133MHz і один PCI-Express x8. Використовуючи розширення, ми можемо додати нові функції, необхідні для роботи.

Віддалене керування сервером PowerEdge 2950 здійснюється через функціональну плату DRAC5. Так можна віддалено контролювати сервер: живлення, температура та інше.

На даному сервері встановлено систему моніторингу Nagios, що включає в себе 4797 хостів та 9800 сервісів, що зображено на рисунку 4.7.

Рисунок 4.7 Кількість хостів та сервісів, що стоять в моніторингу

З такими характеристиками та при такій кількості хостів та сервісів, що моніторяться за допомогою утиліти htop було виявлено, що значення завантаженості ЦП в середньому приймає значення 5%, при максимальній завантаженності – 10%, як зображенно на рисунку 4.7

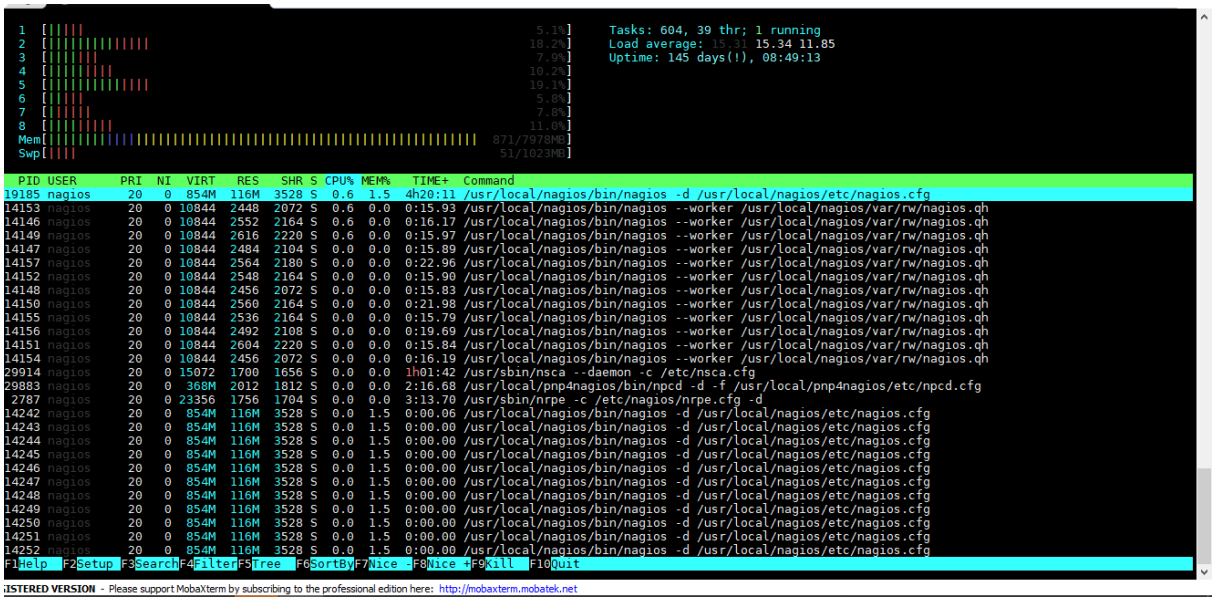

Рисунок 4.7 Виконання утиліти htop на сервері

4.5 Порівняння економічних та експлуатаційних показників при різних типах реалізації системи моніторингу Nagios

4.5.1 Порівняння експлуатаційних показників при різних типах реалізації системи моніторингу Nagios

В своїй роботі для порівняння завантаженості системи я використовувала утиліту htop.

Htop - сучасний монітор процесів, написаний для Linux. Він був створений замінити стандартну програму top. Htop показує динамічний список системних процесів, список вирівнюється за використанням ЦП. В відмінності від top, htop показує всі процеси в системі. Також показує час безперервної роботи, використання процесорів і пам'яті. Htop часто застосовується в тих випадках, коли інформація, що дається утилітою top, недостатня, наприклад при пошуку зменшення пам'яті в процесах. Htop написаний на мові C та використовується для відображення бібліотеки Ncurses.

Тепер пояснимо значення стовпців в утиліті htop:

- PID - ідентифікатор процесу;
- USER - власник процесу;
- PRI - поточний пріоритет (впливає на процесорний час, що відводиться процесу, значення за замовчуванням - 20; чим менше пріоритет, тим більше часу відводиться для процесу, отже він виконується швидше);
- NI - величина зміни пріоритету відносно значення PRI (клавіші F7, F8);
- VIRT - загальний об'єм віртуальної пам'яті, що використовується процесом. Включає в себе: код області (CODE), дані (DATA), розділені бібліотеки (SHARED) і сторінки, переміщені в обмінник пам'яті. Якщо додаток вимагає від ядра виділити йому 100Мб пам'яті, а використовує всього 5 Мб, цей стовпець все рівно буде показувати цифру 100;

- CODE - обсяг пам'яті, містить виконавчий код процесу;
- DATA - об'єм пам'яті, зайнятої даними, використовуваними процесом в ході виконання;
- SWAP - об'єм пам'яті, що використовується процесом, але переміщена в swap-область;
- RES - кількість резидентної пам’яті в кілобайтах. Якщо додаток вимагав від ядра виділити йому 100Мб пам'яті, а використовує всього 5 Мб, то цей стовпець покаже 5;
- SHR - кількість роздільної пам'яті програми в кілобайтах. Це пам'ять, яка може бути використана іншими додатками;
- S – стан сну;
- R - стан виконання;
- D - стан очікування;
- CPU% - використання процесора в відсотковому відношенні;
- MEM% - використання процесу пам'яті в відсотковому відношенні;
- TIME + - час роботи процесу;

При встановленні htop на тестовий макет з Raspberry Pi я отримала показники близькі до значень на рисунку 4.8.

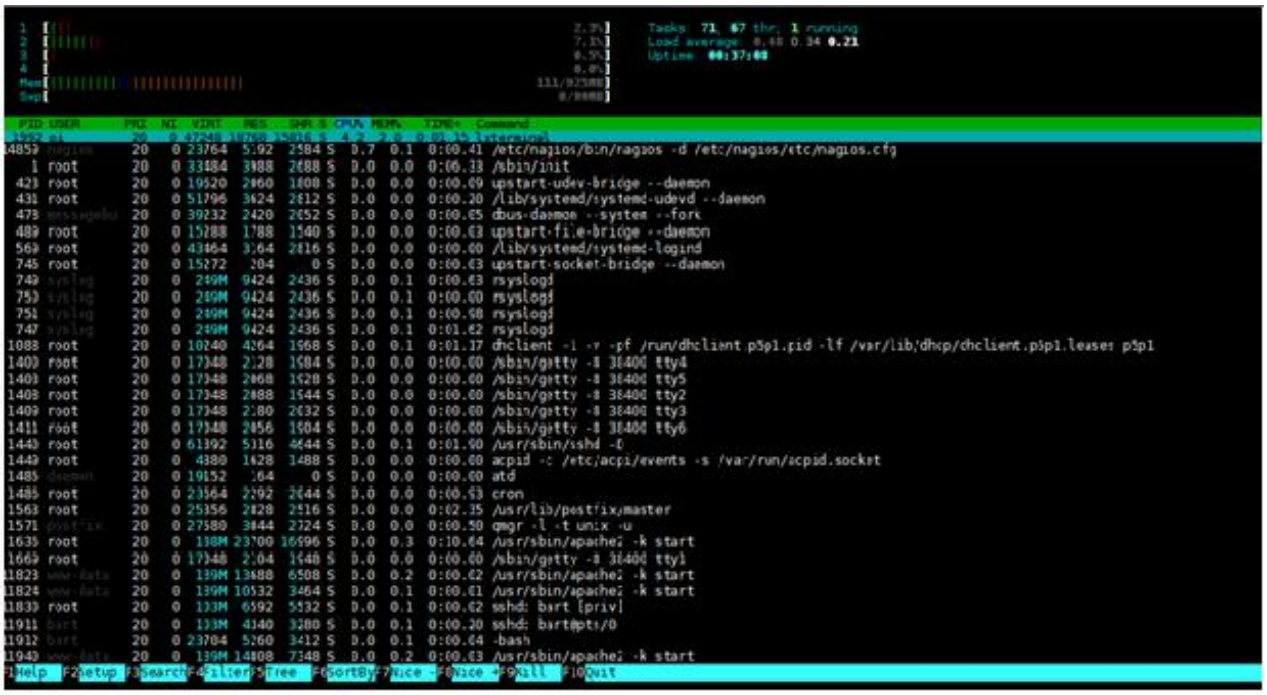

Рисунок 4.8 Виконання утиліти htop на комп’ютері

Максимальне значення завантаженості ЦП яке досягалось в htop це 4.5%, при встановленні в моніторинг 200 хостів та 200 сервісів.

При клонуванні хостів до кількості в 3000 та такої ж кількості сервісів я отримала середнє значення завантаженості ЦП – близьке до 30%, що зображено на рисунку 4.9.

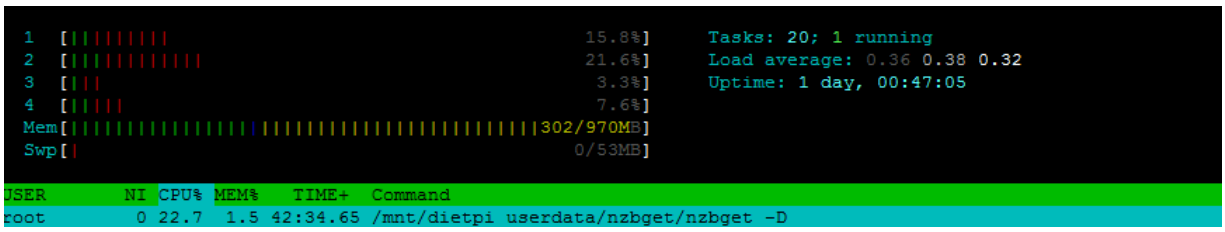

Рисунок 4.9 Виконання утиліти htop на комп’ютері

При встановленні htop на тестовий макет з сервером я отримала показники близькі до значень на рисунку 4.10.

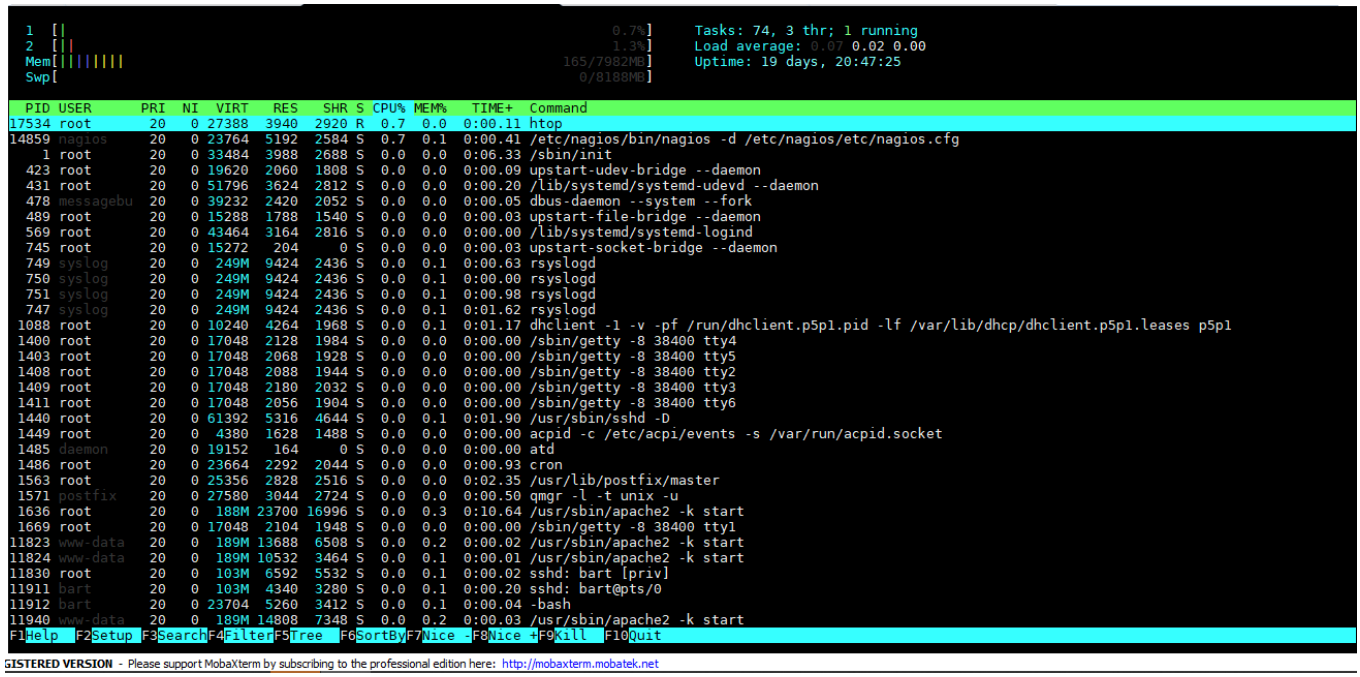

Рисунок 4.10 Виконання утиліти htop на сервері

Максимальне значення завантаженості ЦП яке досягалось в htop це 3%, при встановленні в моніторинг 200 хостів та 200 сервісів.

При клонуванні хостів до кількості в 3000 та такої ж кількості сервісів я отримала середнє значення завантаженості ЦП – близьке до 15%.

При встановленні htop на сервер компанії Інтернет-провайдера WNET я отримала показники близькі до значень на рисунку 4.11- 4.12.

В Nagios на сервері в моніторинг встановлено 4797 хостів та 9800 сервісів і при цьому середнє значення в htop завантаженості ЦП – 5%, а максимальне значення – 12%.

Загальним висновком з отриманих значень ми можемо зробити те, що комп’ютер Raspberry Pi може цілком впоратись з завдання моніторингу мережі. Хоч і показники при навантаженні системи були гіршими в порівнянні з серверами, але ми бачимо, що вони не критичні.

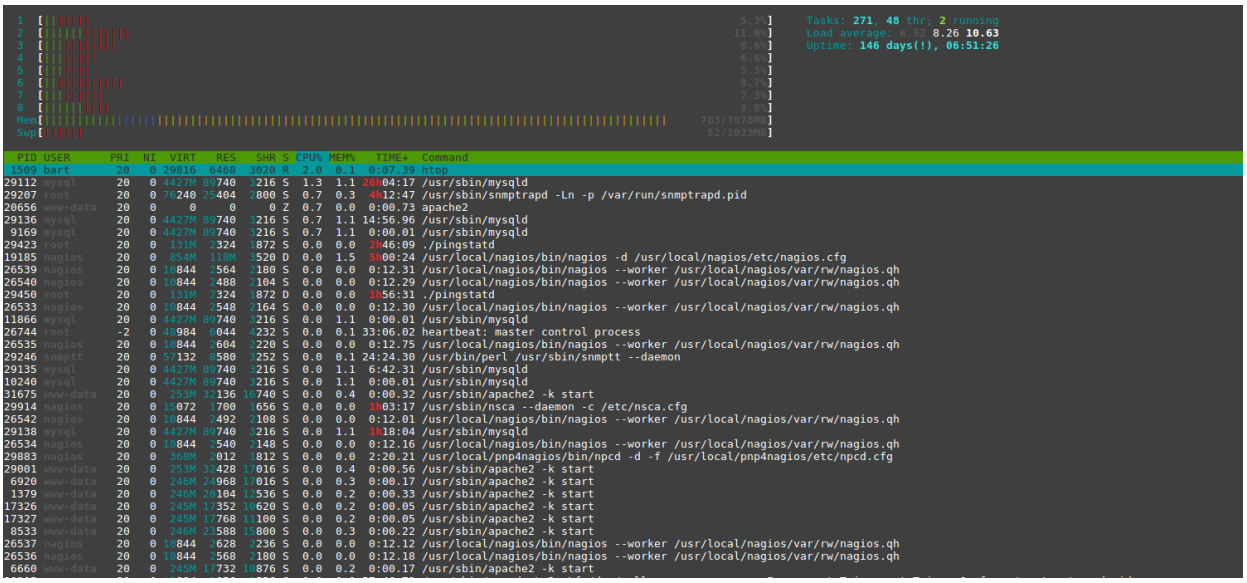

Рисунок 4.11 Виконання утиліти htop на сервері

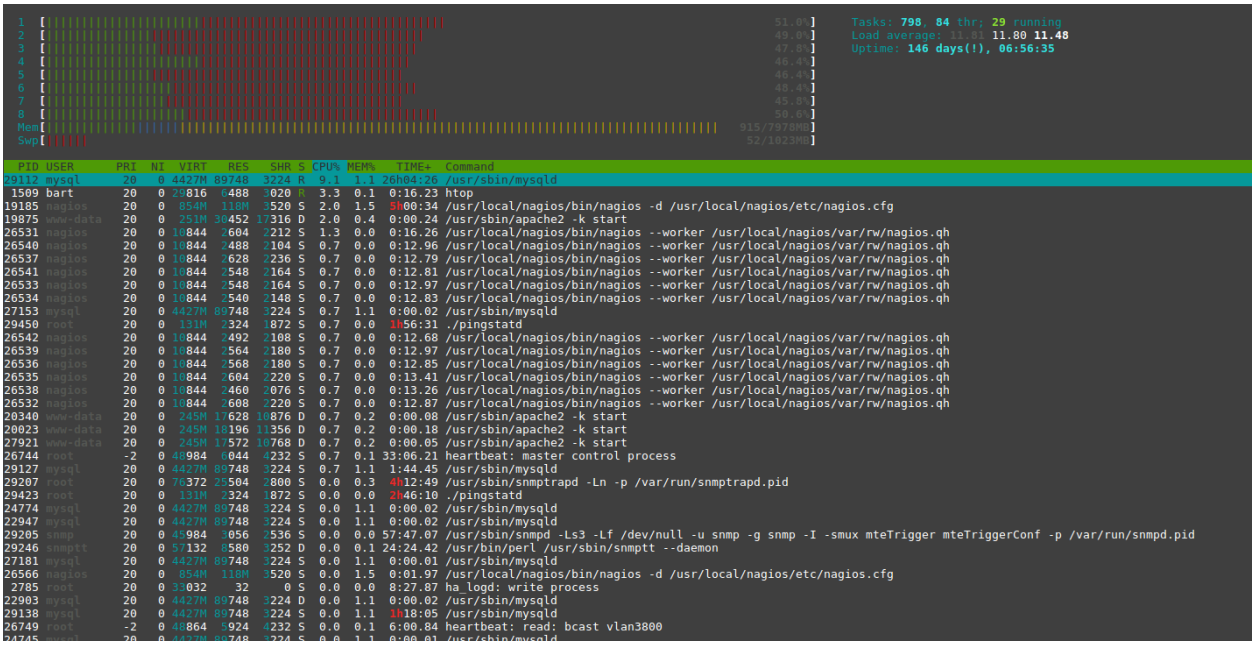

Рис. 4.12 Виконання утиліти htop на сервері

4.5.2 Порівняння економічних показників при різних типах реалізації системи моніторингу Nagios

Порівняння економічних показників приведено в таблиці 4.4.

Таблиця 4.4 Порівняння економічних показників при різних реалізаціях веб-монітору

Raspberry Pi 3 Model B+	$ 35
HP Proliant DL120 G5	$ 300-500
DELL PowerEdge 2950	$ 600-800

Як бачимо Raspberry Pi 3 значно виграє в ціні.

4.6 Висновки до розділу 5

У даному розділі було:

1. Вибрано та описано основний елемент – Raspberry Pi 3 Model B+, що використовується про створенні макета. Описано схему встановлення системи моніторингу на вузол.

2. Вибрано та описано основний елемент – HP Proliant DL120 G5, що використовується про створенні макета. Описано схему встановлення системи моніторингу на вузол.

3. Описано сервер DELL PowerEdge 2950, що встановлеий та використовується в провайдера телекомунікаційних послуг. Проаналізовано роботу програми Nagios на ньому.

4. Зроблено порівняльний аналіз системи моніторингу при двох реалізаціях, їх економічних та експлуатаційних показників.

ВИСНОВКИ

В ході роботи було проведено аналіз щодо будови центрів обробки даних:

- Розглянуто складові центрів обробки даних.
- Розглянуто основні топології побудови ЦОД.
- Перечислено основні недоліки ЦОД.

Центр обробки даних (ЦОД), – це комплексне організаційно-технічне рішення, призначене для створення високопродуктивної і відмовостійкої інформаційної інфраструктури.

Обов'язкові компоненти, що входять до складу ЦОД, можна розділити на три основні групи: технічні компоненти, програмне забезпечення, організаційне середовище.

Серед основних недоліків ЦОД виділяються наступні: складна архітектура, високий відсоток відмов; складне обслуговування і керування; недостатність ресурсів віртуалізації; недостатність ресурсів, неефективне використання кросування; значні потреби в продуктивності та ємності.

В наступному розділі роботи було проведено аналіз та порівняння існуючих систем моніторингу.

Система моніторингу – група пристроїв та програмне забезпечення, що забезпечує систематичний збір і обробку інформації, яка може бути використана для поліпшення процесу прийняття рішення, а також, побічно, для інформування громадськості або прямо як інструмент зворотного зв'язку з метою здійснення проектів, оцінки програм або вироблення політики.

Основні функції систем моніторингу:

- виявляє стан критичних або знаходяться в стані зміни явищ навколишнього середовища, щодо яких буде вироблений курс дій на майбутнє;

- встановлює відносини зі своїм оточенням, забезпечуючи зворотний зв'язок, щодо попередніх успіхів і невдач певної політики або програм;
- встановлює відповідності правилам і контрактним зобов'язанням.

В третьому розділі роботи було вибрано та описано основний елемент – Raspberry Pi, що використовується при створенні макета, вибрано та описано систему моніторингу Nagios, що використовувались при створенні макета.

Raspberry Pi - це мініатюрна, і зручна платформа швидкої розробки електронних пристроїв для новачків і професіоналів, розміром з кредитну карту, ультра дешевий комп'ютер, створений Девідом Брабеном.

Виділено наступні основні перевагі одноплатних комп’ютерів:

- Висока продуктивність.
- Малі габарити.
- Низька собівартість.
- Простота налаштування.
- Можливість використання великого числа додаткових модулів.

Виділено основні можливості, недоліки та переваги системи моніторингу Nagios:

- Моніторинг мережевих служб (SMTP, POP3, HTTP, NNTP, ICMP, SNMP);
- Моніторинг стану хостів (завантаження процесора, використання диска, системні логи);
- Підтримка віддаленого моніторингу через шифровані тунелі SSH або SSL;
- Проста архітектура модулів розширень (плагінів) дозволяє, використовуючи будь-яку мову програмування за вибором (Shell, C ++, Perl, Python, PHP, C # та інші), легко розробляти свої власні способи перевірки служб;
- Паралельна перевірка служб;

- Можливість визначати ієрархії хостів мережі за допомогою «батьківських» хостів, дозволяє виявляти і розрізняти хости, які вийшли з ладу, і ті, які недоступні;
- Відправлення сповіщень у разі виникнення проблем зі службою або хостом (за допомогою пошти, пейджера, смс, або будь-яким іншим способом, визначеним користувачем через модуль системи);
- Можливість визначати обробники подій, що відбулися зі службами або хостами для проактивного вирішення проблем;
- Автоматична ротація лог-файлів;
- Можливість організації спільної роботи декількох систем моніторингу з метою підвищення надійності і створення розподіленої системи моніторингу;

В четвертому розділі роботи було вибрано та описано основний елемент – Raspberry Pi 3 Model B+, що використовується про створенні макета. Описано схему встановлення системи моніторингу на вузол. Обрано та описано основний елемент – HP Proliant DL120 G5, що використовується про створенні макета. Описано схему встановлення системи моніторингу на вузол. Описано сервер DELL PowerEdge 2950, що встановлеий та використовується в провайдера телекомунікаційних послуг WNET. Проаналізовано роботу програми Nagios на ньому. В цьому ж розділі було проведено випробування розробленого макету, наведено порівняння економічних та експлуатаційних показників при двох різних реалізаціях системи моніторингу.

У висновку дійшли до того, що реалізація системи моніторингу цілком можлива на комп’ютері Raspberry Pi, має прийнятні технічні характеристики та має значний виграш у економічних показниках.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Inc. staff (2010), How to Choose a Data Center, retrieved 2012-07-21
2. Центры обработки данных [Електронний ресурс] – Режим доступу до ресурсу: http://www.tadviser.ru/index.php
3. Greenberg A. What Goes Into a Data Center / A. Greenberg, D. Maltz..
4. A. Greenberg et al., “VL2: A scalable and flexible data center network” ACM SIGCOMM Comput. Commun. Rev., vol. 39, no. 4, pp. 51–62, Oct. 2009.
5. C. Guo, H. Wu, K. Tan, L. Shi, Y. Zhang, and S. Lu, “DCell: A scalable and fault-tolerant network structure for data centers,” ACM SIGCOMM Comput. Commun. Rev., vol. 38, no. 4, pp. 75–86, Oct. 2008.
6. Hung LeHong, Jackie Fenn. Key Trends to Watch in Gartner 2012 Emerging Technologies Hype Cycle
7. Cisco Systems, Inc., "Enterprise Campus 3.0 Architecture: Overview and Framework," 2008. [Електронний ресурс] – Режим доступу до ресурсу: http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/campover.html.
8. J. Case, M. Fedor, M. Schoffstall and J. Davin, "RFC1157: A Simple Network Management Protocol (SNMP)," 5 1990. [Електронний ресурс] – Режим доступу до ресурсу: http://www.ietf.org/rfc/rfc1157.txt.
9. Офіційний сайт APC [Електронний ресурс] – Режим доступу до ресурсу: http://www.apc.com/ua/ru/
10. Офіційний сайт Vutlan [Електронний ресурс] – Режим доступу до ресурсу: http://www.vutlan.com/ru/
11. Smith H. Data Center Storage / Hubbert Smith..
12. Kochlan, M.; Hodon, M.; Cechovic, L.; Kapitulik, J.; Jurecka, M., “WSN for traffic monitoring using Raspberry Pi board,” Computer Science and Information Systems (FedCSIS), 2014 Federated Conference on, vol., no., pp.1023,1026.
13. Alpha boards in manufacture Raspberry Pi Foundation [Електронний ресурс] – Режим доступу до ресурсу: https://www.raspberrypi.org/blog/alpha-boards-in-manufacture/

14. Nagios. (n.d.). [Електронний ресурс] – Режим доступу до ресурсу: http://nagios.org.
15. Sophon Mongkolluksamee, Panita Pongpaibool, Chavee Issariyapat, “Strengths and Limitations of Nagios as a Network Monitoring Solution” Proceedings of the 7th International Joint Conference on Computer Science and Software Engineering (JCSSE 2010) Vol. 1, pp. 96-101, Bangkok, Thailand, May 2010
16. Ahmed D. Kora and Moussa Moindze Soidridine, “Nagios based enhanced IT management system,” Interntional Journal of Engineering Science and Technology, vol. 4, no. 3, pp. 818–822, 2012.
17. SpringGraph Flex Component. (n.d). [Електронний ресурс] – Режим доступу до ресурсу: http://markshepherd.com/SpringGraph/
18. NSClient++ for Windows, Secure monitoring daemon, Retrieved December 2012). [Електронний ресурс] – Режим доступу до ресурсу: http://www.nsclient.org/nscp/wiki/doc/about/0.4.x
19. D. Doug, B. James R., M. High, “Best of open source networking software,”infoworld.com, Aug 31, 2009.
20. Сервер HP ProLiant DL120 G5 [Електронний ресурс] – Режим доступу до ресурсу: https://support.hpe.com/hpsc/doc/public
21. Сервер Dell PowerEdge 2950 [Електронний ресурс] – Режим доступу до ресурсу: https://s4u.com.ua/dell-poweredge-29502.html